**IN THE UNITED STATES DISTRICT COURT**
**DISTRICT OF CONNECTICUT**

| | |
|---|---|
| CINDY ROUGEAU, *et al.*, individually and on behalf of all others similarly situated,<br><br>Plaintiffs,<br><br>v.<br><br>AETNA INC.; and AETNA LIFE INSURANCE COMPANY,<br><br>Defendants | Case No. 3:23-cv-00635-KAD<br><br>**CONSOLIDATED CLASS ACTION COMPLAINT**<br><br>**JURY TRIAL DEMANDED** |

Plaintiffs Cindy Rougeau, Beverly Banks, Mark Brewer, Randall Carter, Nigel Keep, Vincentina Luciano, David Mueller, Jeanne Peffley-Wilson, Roberta Platt, Michelle Ronne, Gordon Titcomb, Roderick Veazey, Nicholas Venezia, Valarie Venezia, Donna Vogel, and John Vogel (collectively, "Plaintiffs"), individually and on behalf of all others similarly situated, assert the following against Defendants Aetna Inc. and Aetna Life Insurance Company (collectively, "Aetna"), based on Plaintiffs' personal knowledge, investigation of counsel, facts of public record, and information and belief as to all other matters.

## NATURE OF THE ACTION

1. This class action arises out of Aetna's abdication of the duties it owes millions of Aetna health plan holders to safeguard their sensitive, personally identifiable information ("PII") and protected health information ("PHI").

2. Aetna health plan holders, such as Plaintiffs and Class Members (defined below), entrusted PII and PHI to Aetna and permitted Aetna to gather their PII and PHI in connection with the health plans Plaintiffs purchased from Aetna and the medical treatments they sought coverage

for pursuant to those health plans. This entrustment was made in confidence with the reasonable expectation that Aetna would fulfill its duties and obligations to safeguard their PII and PHI.

3. Plaintiffs expected Aetna to comply with federal and state law and to, *inter alia*, implement and execute safeguards that would ensure that: (i) Aetna's health plan holders' PII and PHI is stored and transmitted securely; (ii) Aetna would only share its health plan holders' PII and PHI when necessary; and (iii) Aetna would notify its health plan holders promptly if their information was compromised due to, among other things, unauthorized access.

4. But Aetna failed to fulfill its basic legal duties and obligations. And because of Aetna's failures, between January 30 and February 7, 2023, unauthorized third parties gained access to the PII and PHI of millions of Aetna health plan holders, including their names, genders, health plan subscriber numbers, Medicare numbers, addresses, phone numbers, dates of birth, and social security numbers (the "Data Breach" or "Breach").[1] This data is recognized as valuable by many different constituencies, including: (i) Aetna itself; (ii) the cybercriminals who exfiltrated the PII and PHI for purposes of selling it to others who intend to commit identity theft and fraud; and (iii) Plaintiffs and Class Members, whose PII and PHI were stolen.

5. The unauthorized party gained access to Plaintiffs' and Class Members' PII and PHI by accessing the servers of a company known as NationsBenefits, a vendor Aetna hired to provide hearing aid and fringe Medicare benefits to a fraction of eligible Aetna health plan holders. Pursuant to this arrangement, Aetna affirmatively transferred the PII and PHI of millions of Aetna health plan holders to NationsBenefits, despite the fact that the overwhelming majority of Class Members did not use the services that NationsBenefits provides and never would. In fact, prior to

[1] *Data Breach Notifications, NationsBenefits Holdings, LLC*, OFF. OF THE ME ATT'Y GEN., https://apps.web.maine.gov/online/aeviewer/ME/40/cc06cdee-0715-4eea-8b33-c391dba8fe5e.shtml (last accessed on Sept. 18, 2023).

this breach, ***no Plaintiff was even aware of the existence of NationsBenefits let alone the fact that NationsBenefits possessed their PII and PHI***. (Emphasis added.) As such, NationsBenefits was not authorized to obtain Plaintiffs' and Class Members' PII and PHI from Aetna, and Aetna had no legitimate business reason to provide Plaintiffs' and Class Members' PII and PHI to NationsBenefits, yet Aetna did so affirmatively without their consent.

6. Upon information and belief, the unauthorized third party that perpetrated the Data Breach are cybercriminals part of a Russian-linked hacker/ransomware group responsible for numerous other hacking events.[2] Upon information and belief, the unauthorized third party carried out the Data Breach for the purpose of engaging in identity theft to the detriment and injury of Plaintiffs and Class Members. Upon information and belief, this unauthorized third party already has begun to leak Plaintiffs' and Class Members' PII and PHI.[3]

7. Exacerbating the harm caused by the Data Breach, Aetna health plan holders, such as Plaintiffs, were not informed of the Data Breach for nearly three months after it occurred. It was not until April 27, 2023, that millions of Aetna health plan holders were mailed letters informing them that their sensitive PII and PHI had been compromised. Even then, the notice was provided by NationsBenefits, and not Aetna. To date, upon information and belief, ***Aetna has not communicated with Aetna health plan holders at all regarding the Data Breach***. (Emphasis added.)

---

[2] Jessica David, *Clop ransomware hack of Fortra GoAnywhere MFT hits 1M CHS patients*, SC MEDIA (Feb. 15, 2023), https://www.scmagazine.com/news/ransomware/clop-ransomware-hack-of-fortra-goanywhere-mft-hits-1m-chs-patients; *HHS: Russia-linked ransomware group claims continued health care attacks*, AM. HOSP. ASS'N (Feb. 23, 2023), https://www.aha.org/news/headline/2023-02-23-hhs-russia-linked-ransomware-group-claims-continued-health-care-attacks.

[3] Lawrence Abrams, *Clop now leaks data stolen in MOVEit attacks on clearweb sites*, BLEEPINGCOMPUTER (July 23, 2023), https://www.bleepingcomputer.com/news/security/clop-now-leaks-data-stolen-in-moveit-attacks-on-clearweb-sites/.

8. Aetna has a duty to safeguard and protect health plan holder information entrusted to it and could have prevented this theft had it limited the customer information it shared with its business associates and employed reasonable measures to ensure its business associates, such as NationsBenefits, implemented and maintained adequate data security measures and protocols in order to secure Aetna health plan holders' PII and PHI.

9. Upon information and belief, prior to and through the date of the Data Breach, Aetna obtained Plaintiffs' and Class Members' PII and PHI, maintained that sensitive data in a negligent and/or reckless manner, and failed to prevent its business associates, such as NationsBenefits, from doing the same.

10. As a result of Aetna's negligent and/or reckless conduct and affirmative acts, Plaintiffs and Class Members now suffer from a heightened and imminent risk of fraud and identity theft and must constantly monitor their financial accounts. Plaintiffs and Class Members also will likely suffer additional financial costs for purchasing necessary credit monitoring services, credit freezes, credit reports, and other protective measures to deter and detect identity theft.

11. Plaintiffs and Class Members have suffered – and will continue to suffer – from the loss of the benefit of their bargain, unexpected out-of-pocket expenses, lost or diminished value of their PII and PHI, emotional distress, the value of their time reasonably incurred to mitigate the fallout of the Data Breach, nominal damages, and are under a current and continuous threat of having their PII and PHI exploited to their detriment for gain by cybercriminals.

12. Plaintiffs thus bring this class action against Aetna for the injuries Aetna inflicted on Plaintiffs and millions[4] of similarly situated persons ("Class Members") due to, among other

[4] *Cases Currently Under Investigation*, U.S. DEP'T OF HEALTH & HUM. SERVS., https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed on Sept. 18, 2023).

things, Aetna's: (i) failure to properly secure and safeguard highly valuable PII and PHI, including without limitation, names, addresses, emails, phone numbers, health plan account and ID numbers, dates of birth, and Medicare numbers, in particular when sharing and transmitting that data to its vendors and business associates; (ii) failure to comply with statutes, regulations, and industry standards to protect information systems that contain PII and PHI; (iii) unlawful, affirmative disclosure of the PII and PHI of Plaintiffs and Class Members to NationsBenefits who was not authorized to receive that information; and (iv) failure to provide adequate notice to Plaintiffs and Class Members that their PII and PHI had been disclosed and compromised.

13. Plaintiffs, on behalf of themselves and all others similarly situated, bring claims for negligence, negligence *per se*, breach of contract, unjust enrichment, breach of confidence, and violations of consumer protection statutes, and a request for equitable relief and a declaratory judgment.

14. Plaintiffs seek remedies including, but not limited to, compensatory damages, treble damages, punitive damages, nominal damages, reimbursement of out-of-pocket costs, and injunctive relief requiring Aetna to, *inter alia*: (i) adopt reasonably sufficient practices to safeguard the PII and PHI in Aetna's custody and control; (ii) cease transmitting PII and PHI to third-party business associates absent a legitimate business purpose for doing so; and (iii) to properly verify, monitor, and audit that the data security measures of third-party business associates are adequate to protect the PII and PHI that Aetna transmits to them.

15. Given that information relating to the Data Breach remains exclusively in Aetna's control, Plaintiffs anticipate that additional information in support for their claims will emerge during discovery.

## JURISDICTION AND VENUE

16. This Court has original jurisdiction under the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. §1332(d)(2), because the amount in controversy for the Class exceeds the sum of $5,000,000, exclusive of interest and costs, there are more than 100 Class Members, and minimal diversity exists because many Plaintiffs and many Class Members are citizens of a different state than Aetna.

17. This Court has general personal jurisdiction over Aetna because Aetna's principal place of business and headquarters is in this District, in Hartford, Connecticut. Aetna also regularly conducts substantial business in this District.

18. Venue is proper in this District under 28 U.S.C. §1391(b) because a substantial part of the events giving rise to the claims emanated from activities within this District, and Aetna conducts substantial business in this District.

## PARTIES

### A. Plaintiffs

**Plaintiff Cindy Rougeau**

19. Plaintiff Cindy Rougeau ("Plaintiff Rougeau") is a citizen and resident of New York.

20. Plaintiff Rougeau has maintained health insurance coverage through Aetna. Aetna required Plaintiff Rougeau to provide her PII and PHI to Aetna in order to receive health insurance benefits and other services from Aetna. Upon information and belief, Aetna provided Plaintiff Rougeau's PII and PHI to NationsBenefits after she enrolled with Aetna.

21. Plaintiff Rougeau received a letter dated April 27, 2023, notifying Plaintiff Rougeau that as a health plan holder of Aetna her first name, last name, gender, health plan

subscriber identification number, address, phone number, date of birth, and Medicare number were compromised in the Data Breach.

22. Shortly after and as a result of the Data Breach, Plaintiff Rougeau was the victim of fraud and identity theft. Specifically, she experienced a large increase in spam and suspicious phone calls, texts, and emails from strangers where she was asked to provide personal information, join alleged social media groups, or click on weblinks. In addition, she received a call from Target regarding a credit card she purportedly opened, although Plaintiff Rougeau never had applied for such a credit card. An unidentified charge for apparel from a concert in Jones Beach, New York also appeared on Plaintiff Rougeau's credit card statement shortly after the Data Breach, even though she never has visited Jones Beach. Plaintiff Rougeau also received a letter from a likely fraudster claiming to be the IRS seeking to obtain Plaintiff Rougeau's personal information. Similarly, Plaintiff Rougeau became aware that hackers had unsuccessfully tried to gain access to her email account approximately 93 times. Indeed, Equifax recently informed Plaintiff Rougeau that her confidential information is on the dark web. Aetna even contacted Plaintiff Rougeau about apparent unauthorized attempts to receive medication using Plaintiff Rougeau's name through doctors that Plaintiff Rougeau has never seen as a patient.

23. As a result of the Data Breach and as recommended in the Notice, Plaintiff Rougeau made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, closely reviewing financial statements, logging into online accounts to check activity, obtaining her credit report from the credit reporting agencies, freezing her credit, signing up for credit monitoring, and continually monitoring her credit information. Plaintiff Rougeau has spent significant time, approximately 50 hours, responding to the Data Breach and will continue to spend valuable time she otherwise would have spent on other activities, including

but not limited to work and/or recreation. Plaintiff Rougeau suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced increased concerns regarding the loss of her privacy as well as anxiety and weight loss over the impact of cybercriminals accessing and using her PII and PHI.

24. Plaintiff Rougeau believed that Aetna would protect her PII and PHI once she provided it to Aetna. Plaintiff Rougeau would not have enrolled with Aetna if she had known Aetna would not adequately protect her PII and PHI.

25. Thus, as a result of the Data Breach, Plaintiff Rougeau has faced and continues to face a present and continuing risk of fraud and identity theft for her lifetime. Plaintiff Rougeau has a continuing interest in ensuring that her PII and PHI, which upon information and belief remains backed up in Aetna's possession, is protected and safeguarded from future data breaches.

**Plaintiff Beverly Banks**

26. Plaintiff Beverly Banks ("Plaintiff Banks") is a citizen and resident of Michigan.

27. Plaintiff Banks has maintained health insurance coverage through Aetna. Aetna required Plaintiff Banks to provide her PII and PHI to Aetna in order to receive health insurance benefits and other services from Aetna. Upon information and belief, Aetna provided Plaintiff Banks's PII and PHI to NationsBenefits after she enrolled with Aetna.

28. Plaintiff Banks received a letter dated April 27, 2023, notifying Plaintiff Banks that as a health plan holder of Aetna her first name, middle initial, last name, gender, health plan subscriber identification number, address, phone number, date of birth, and Medicare number were compromised in the Data Breach.

29. Shortly after and as a result of the Data Breach, Plaintiff Banks was the victim of fraud and identity theft. Specifically, she experienced a large increase in spam and suspicious

phone calls, texts, and emails from strangers where she is asked to provide personal information, press a number to continue, or click on weblinks, resulting in her needing to shut her phone off. In addition, she received an alert through her Experian account regarding an "account inquiry" or "credit card inquiry," which she did not request. Indeed, Equifax recently informed Plaintiff Banks that her confidential information is on the dark web.

30. As a result of the Data Breach and as recommended in the Notice, Plaintiff Banks made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, calling Aetna and/or NationsBenefits regarding more information about this Data Breach, and continually monitoring her credit information. Plaintiff Banks has spent significant time, approximately 11 hours, responding to the Data Breach and will continue to spend valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. Plaintiff Banks suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced anxiety and increased concerns regarding the loss of her privacy, including spending about 20 hours coping with anxiety and emotional anguish, over the impact of cybercriminals accessing and using her PII and PHI.

31. Plaintiff Banks believed that Aetna would protect her PII and PHI once she provided it to Aetna. Plaintiff Banks would not have enrolled with Aetna if she had known Aetna would not adequately protect her PII and PHI.

32. Thus, as a result of the Data Breach, Plaintiff Banks has faced and continues to face a present and continuing risk of fraud and identity theft for her lifetime. Plaintiff Banks has a continuing interest in ensuring that her PII and PHI, which upon information and belief remains backed up in Aetna's possession, is protected and safeguarded from future data breaches.

**Plaintiff Mark Brewer**

33. Plaintiff Mark Brewer ("Plaintiff Brewer") is a citizen and resident of Oklahoma.

34. Plaintiff Brewer has maintained health insurance coverage through Aetna. Aetna required Plaintiff Brewer to provide his PII and PHI to Aetna in order to receive health insurance benefits and other services from Aetna. Upon information and belief, Aetna provided Plaintiff Brewer's PII and PHI to NationsBenefits after he enrolled with Aetna.

35. Plaintiff Brewer received a letter dated April 27, 2023, notifying Plaintiff Brewer that as a health plan holder of Aetna his first name, last name, gender, health plan subscriber identification number, address, phone number, date of birth, and Medicare number were compromised in the Data Breach.

36. Shortly after and as a result of the Data Breach, Plaintiff Brewer was the victim of fraud and attempted identity theft. Specifically, he experienced a large increase in spam phone calls and suspicious text messages from strangers trying to solicit a response, including someone posing as a representative of UnitedHealthcare asking for sensitive personal information after he signed up for his new insurance plan. Plaintiff Brewer confirmed with the real UnitedHealthcare that this was a fraudulent call.

37. As a result of the Data Breach and as recommended in the Notice, Plaintiff Brewer made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, freezing his credit through Equifax, and calling and emailing NationsBenefits and Aetna directly to find out more about the Data Breach. Plaintiff Brewer has spent significant time, including 3-4 hours of phone calls, responding to the Data Breach and will continue to spend valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. Plaintiff Brewer suffered lost time, annoyance, interference,

and inconvenience as a result of the Data Breach and has experienced anger and increased concerns regarding the loss of his privacy and potential further damages over the impact of cybercriminals accessing and using his PII and PHI. Plaintiff Brewer is also concerned that because he lives on a month-to-month check, he likely will not have the time or resources to deal with any potential financial fraud that could occur as a result of the Data Breach. Furthermore, Plaintiff Brewer is upset and concerned that Aetna was not transparent about the third parties that it shared health plan holders' data with as well as the lack of professionalism of the agent who dismissed Plaintiff Brewer's requests for information and laughed at him before directing him to a useless phone number, including a number for a moving company, when he called to speak to Aetna and NationsBenefits about the Data Breach.

38. Plaintiff Brewer believed that Aetna would protect his PII and PHI once he provided it to Aetna. Plaintiff Brewer would not have enrolled with Aetna if he had known Aetna would not adequately protect his PII and PHI.

39. Thus, as a result of the Data Breach, Plaintiff Brewer has faced and continues to face a present and continuing risk of fraud and identity theft for his lifetime. Plaintiff Brewer has a continuing interest in ensuring that his PII and PHI, which upon information and belief remains backed up in Aetna's possession, is protected and safeguarded from future data breaches.

**Plaintiff Randall Lynn Carter**

40. Plaintiff Randall Lynn Carter ("Plaintiff Carter") is a citizen and resident of Oklahoma.

41. Plaintiff Carter has maintained health insurance coverage through Aetna. Aetna required Plaintiff Carter to provide his PII and PHI to Aetna in order to receive health insurance benefits and other services from Aetna. Upon information and belief, Aetna provided Plaintiff

Carter's PII and PHI to NationsBenefits after he enrolled with Aetna.

42. Plaintiff Carter received a letter dated April 27, 2023, notifying Plaintiff Carter that as a health plan holder of Aetna his first name, middle initial, last name, gender, health plan subscriber identification number, address, phone number, date of birth, and Medicare number were compromised in the Data Breach.

43. Shortly after and as a result of the Data Breach, Plaintiff Carter was the victim of fraud. Specifically, he experienced a large increase in spam and suspicious phone calls, texts, and emails from strangers, including frequent calls requiring Plaintiff Carter to "press one to continue."

44. As a result of the Data Breach and as recommended in the Notice, Plaintiff Carter made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to, researching the Data Breach, closely reviewing financial statements, logging into online accounts to check activity, obtaining his credit report from the credit reporting agencies, freezing his credit, and continually monitoring his credit information. Plaintiff Carter has spent significant time, including over four hours calling Aetna and/or NationsBenefits, responding to the Data Breach and will continue to spend valuable time he otherwise would have spent on other activities, including but not limited to, work and/or recreation. Plaintiff Carter suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced anxiety and increased concerns regarding the loss of his privacy as well as anxiety over the impact of cybercriminals accessing and using his PII and PHI, stating his medication intake has gone up as a result. Plaintiff Carter believes the stress and anxiety will likely cause him to end up in the hospital.

45. Plaintiff Carter believed that Aetna would protect his PII and PHI once he provided it to Aetna. Plaintiff Carter would not have enrolled with Aetna if he had known Aetna would not adequately protect his PII and PHI.

46. Thus, as a result of the Data Breach, Plaintiff Carter has faced and continues to face a present and continuing risk of fraud and identity theft for his lifetime. Plaintiff Carter has a continuing interest in ensuring that his PII and PHI, which upon information and belief remains backed up in Aetna's possession, is protected and safeguarded from future data breaches.

**Plaintiff Nigel Keep**

47. Plaintiff Nigel Keep ("Plaintiff Keep") is a citizen and resident of Nevada.

48. Plaintiff Keep has maintained health insurance coverage through Aetna. Aetna required Plaintiff Keep to provide his PII and PHI to Aetna in order to receive health insurance benefits and other services from Aetna. Upon information and belief, Aetna provided Plaintiff Keep's PII and PHI to NationsBenefits after he enrolled with Aetna.

49. Plaintiff Keep received a letter dated April 27, 2023, notifying Plaintiff Keep that as a health plan holder of Aetna his first name, middle initial, last name, gender, health plan subscriber identification number, address, phone number, and date of birth were compromised in the Data Breach.

50. Shortly after and as a result of the Data Breach, Plaintiff Keep was the victim of fraud and possible attempted identity theft. Specifically, he experienced a large increase in spam and suspicious phone calls, texts, and emails from strangers where he is requested to contact the sender or to click on a link. In addition, dark web scans indicate some of his information is on the dark web.

51. As a result of the Data Breach and as recommended in the Notice, Plaintiff Keep made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, closely reviewing financial statements, logging into online accounts to check activity, obtaining his credit report from the credit reporting agencies, continually monitoring his credit information, and periodically doing dark web searches for his information. Plaintiff Keep has spent significant time, approximately 1-2 hours each month and over two hours on the phone with Aetna or NationsBenefits, responding to the Data Breach and will continue to spend valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. Plaintiff Keep suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced a constant "state of vigilance" and concern that his financial security could be destroyed over the impact of cybercriminals accessing and using his PII and PHI.

52. Plaintiff Keep believed that Aetna would protect his PII and PHI once he provided it to Aetna. Plaintiff Keep would not have enrolled with Aetna if he had known Aetna would not adequately protect his PII and PHI.

53. Thus, as a result of the Data Breach, Plaintiff Keep has faced and continues to face a present and continuing risk of fraud and identity theft for his lifetime. Plaintiff Keep has a continuing interest in ensuring that his PII and PHI, which upon information and belief remains backed up in Aetna's possession, is protected and safeguarded from future data breaches.

**Plaintiff Vincentina Luciano**

54. Plaintiff Vincentina Luciano ("Plaintiff Luciano") is a citizen and resident of Florida.

55. Plaintiff Luciano has maintained health insurance coverage through Aetna. Aetna required Plaintiff Luciano to provide her PII and PHI to Aetna in order to receive health insurance benefits and other services from Aetna. Upon information and belief, Aetna provided Plaintiff Luciano's PII and PHI to NationsBenefits after she enrolled with Aetna.

56. Plaintiff Luciano received a letter dated April 27, 2023, notifying Plaintiff Luciano that as a health plan holder of Aetna her first name, middle initial, last name, gender, health plan subscriber identification number, address, phone number, and date of birth were compromised in the Data Breach.

57. Shortly after and as a result of the Data Breach, Plaintiff Luciano was the victim of fraud and identity theft. Specifically, she experienced a large increase in spam and suspicious phone calls, texts, and emails from strangers where she is asked to provide personal information, including a call from someone alleging to be Bank of America, where she did provide personal information. In addition, someone fraudulently accessed her Bank of America account, changed the password, and used Zelle to withdraw money between March and July of 2023. While the money was reimbursed and the account frozen for a time, this incident required her to go to the bank in person to withdraw her funds and ultimately switch banks. An unauthorized person also tried to change her account password with TD Ameritrade, but the fraudster's effort was blocked by an alert.

58. As a result of the Data Breach and as recommended in the Notice, Plaintiff Luciano made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, closely reviewing financial and account statements, logging into online accounts to check activity, talking with banks about fraud, freezing her credit, continually monitoring her credit information, and resetting automatic billing instructions and direct deposits.

Plaintiff Luciano plans to sign up for credit monitoring, as well. Plaintiff Luciano has spent significant time, approximately 25 hours, responding to the Data Breach and will continue to spend valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. Plaintiff Luciano suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced increased concerns regarding the loss of her privacy as well as anxiety over the impact of cybercriminals accessing and using her PII and PHI, including general worry and because her bank stated it would deny a loan for home improvements based on the Data Breach.

59. Plaintiff Luciano believed that Aetna would protect her PII and PHI once she provided it to Aetna. Plaintiff Luciano would not have enrolled with Aetna if she had known Aetna would not adequately protect her PII and PHI.

60. Thus, as a result of the Data Breach, Plaintiff Luciano has faced and continues to face a present and continuing risk of fraud and identity theft for her lifetime. Plaintiff Luciano has a continuing interest in ensuring that her PII and PHI, which upon information and belief remains backed up in Aetna's possession, is protected and safeguarded from future data breaches.

**Plaintiff David Mueller**

61. Plaintiff David Mueller ("Plaintiff Mueller") is a citizen and resident of Illinois.

62. Plaintiff Mueller has maintained health insurance coverage through Aetna. Aetna required Plaintiff Mueller to provide his PII and PHI to Aetna in order to receive health insurance benefits and other services from Aetna. Upon information and belief, Aetna provided Plaintiff Mueller's PII and PHI to NationsBenefits after he enrolled with Aetna.

63. Plaintiff Mueller received a letter dated April 27, 2023, notifying Plaintiff Mueller that as a health plan holder of Aetna his first name, middle initial, last name, gender, health plan

subscriber identification number, address, phone number, and date of birth were compromised in the Data Breach.

64. Shortly after and as a result of the Data Breach, Plaintiff Mueller was the victim of fraud and identity theft. Specifically, he experienced a large increase in spam and suspicious phone calls, texts, and emails from strangers asking him to press a number or click a link to continue. In addition, an unauthorized user managed to charge his existing credit card on two separate occasions, resulting in Plaintiff Mueller needing to close a credit card account twice over a two-month period.

65. As a result of the Data Breach and as recommended in the Notice, Plaintiff Mueller made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, constantly monitoring all credit cards, bank accounts, and PayPal account. Plaintiff Mueller has spent significant time, approximately 35 hours (including 1-2 hours on the phone with Aetna and/or NationsBenefits), responding to the Data Breach and will continue to spend valuable time he otherwise would have spent on other activities, including but not limited to, work and/or recreation. Plaintiff Mueller suffered lost time, interference, and inconvenience as a result of the Data Breach and has experienced increased concerns regarding the loss of his privacy as well as anxiety, including four hours a month coping with increased anxiety and emotional anguish, over the impact of cybercriminals accessing and using his PII and PHI. Indeed, Plaintiff Mueller constantly worries about the extensive negative impact the Data Breach could cause him, including but not limited to, fear of someone cleaning out his savings or checking account, FICO credit score decreases, home title theft, and more unauthorized charges.

66. Plaintiff Mueller believed that Aetna would protect his PII and PHI once he provided it to Aetna. Plaintiff Mueller would not have enrolled with Aetna if he had known Aetna would not adequately protect his PII and PHI.

67. Thus, as a result of the Data Breach, Plaintiff Mueller has faced and continues to face a present and continuing risk of fraud and identity theft for his lifetime. Plaintiff Mueller has a continuing interest in ensuring that his PII and PHI, which upon information and belief remains backed up in Aetna's possession, is protected and safeguarded from future data breaches.

**Plaintiff Jeanne Peffley-Wilson**

68. Plaintiff Jeanne Peffley-Wilson ("Plaintiff Peffley-Wilson") is a citizen and resident of Georgia.

69. Plaintiff Peffley-Wilson has maintained health insurance coverage through Aetna. Aetna required Plaintiff Peffley-Wilson to provide her PII and PHI to Aetna in order to receive health insurance benefits and other services from Aetna. Upon information and belief, Aetna provided Plaintiff Peffley-Wilson's PII and PHI to NationsBenefits after she enrolled with Aetna.

70. Plaintiff Peffley-Wilson received a letter dated April 27, 2023, notifying Plaintiff Peffley-Wilson that as a health plan holder of Aetna her first name, last name, gender, health plan subscriber identification number, address, phone number, date of birth, and Medicare number were compromised in the Data Breach.

71. Shortly after and as a result of the Data Breach, Plaintiff Peffley-Wilson was the victim of fraud. Specifically, she experienced several scam emails informing her that her various accounts are being closed and she must respond right away or click a link to prevent further action as well as scam emails posing to be companies such as Amazon. In addition, she received calls

and text messages from strangers asking her to press a number to continue, or to click a link because her accounts are past due.

72. As a result of the Data Breach and as recommended in the Notice, Plaintiff Peffley-Wilson made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, making multiple calls to Aetna and NationsBenefits, closely reviewing financial statements, changing the passwords for all of her accounts, and checking her online account statements at least once per week. Plaintiff Peffley-Wilson has spent significant time, approximately 5-6 hours initially and an additional 1-2 hours each week, responding to the Data Breach and will continue to spend valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. Plaintiff Peffley-Wilson suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced increased concerns regarding the loss of her privacy as well as anxiety, including constantly worrying, over the impact of cybercriminals accessing and using her PII and PHI.

73. Plaintiff Peffley-Wilson believed that Aetna would protect her PII and PHI once she provided it to Aetna. Plaintiff Peffley-Wilson would not have enrolled with Aetna if she had known Aetna would not adequately protect her PII and PHI.

74. Thus, as a result of the Data Breach, Plaintiff Peffley-Wilson has faced and continues to face a present and continuing risk of fraud and identity theft for her lifetime. Plaintiff Peffley-Wilson has a continuing interest in ensuring that her PII and PHI, which upon information and belief remains backed up in Aetna's possession, is protected and safeguarded from future data breaches.

**Plaintiff Roberta Platt**

75. Plaintiff Roberta Platt ("Plaintiff Platt") is a citizen and resident of Massachusetts.

76. Plaintiff Platt has maintained health insurance coverage through Aetna. Aetna required Plaintiff Platt to provide her PII and PHI to Aetna in order to receive health insurance benefits and other services from Aetna. Upon information and belief, Aetna provided Plaintiff Platt's PII and PHI to NationsBenefits after she enrolled with Aetna.

77. Plaintiff Platt received a letter dated April 27, 2023, notifying Plaintiff Platt that as a health plan holder of Aetna her first name, middle initial, last name, gender, health plan subscriber identification number, address, phone number, and date of birth, were compromised in the Data Breach.

78. Shortly after and as a result of the Data Breach, Plaintiff Platt was the victim of spam calls and phishing attempts. Specifically, she experienced a large increase in spam and suspicious phone calls, texts, and emails, such as unsolicited credit card offers.

79. As a result of the Data Breach and as recommended in the Notice, Plaintiff Platt made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to, researching the Data Breach, calling Aetna and NationsBenefits on multiple occasions, calling her banks, and monitoring her accounts. Plaintiff Platt has spent significant time, over five hours, responding to the Data Breach and coping with anxiety, and will continue to spend valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. Plaintiff Platt suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced increased concerns regarding the loss of her privacy as well as anxiety, including worrying about someone using her name to open credit card accounts or loans using her name, over the impact of cybercriminals accessing and using her PII and PHI.

80. Plaintiff Platt believed that Aetna would protect her PII and PHI once she provided it to Aetna. Plaintiff Platt would not have enrolled with Aetna if she had known Aetna would not adequately protect her PII and PHI and is disappointed that Aetna still hasn't contacted its customers directly to inform them of the Data Breach.

81. Thus, as a result of the Data Breach, Plaintiff Platt has faced and continues to face a present and continuing risk of fraud and identity theft for her lifetime. Plaintiff Platt has a continuing interest in ensuring that her PII and PHI, which upon information and belief remains backed up in Aetna's possession, is protected and safeguarded from future data breaches.

**Plaintiff Michelle Ronne**

82. Plaintiff Michelle Ronne ("Plaintiff Ronne") is a citizen and resident of North Dakota.

83. Plaintiff Ronne has maintained health insurance coverage through Aetna. Aetna required Plaintiff Ronne to provide her PII and PHI to Aetna in order to receive health insurance benefits and other services from Aetna. Upon information and belief, Aetna provided Plaintiff Ronne's PII and PHI to NationsBenefits after she enrolled with Aetna.

84. Plaintiff Ronne received a letter dated April 27, 2023, notifying Plaintiff Ronne that as a health plan holder of Aetna her first name, middle initial, last name, gender, health plan subscriber identification number, address, phone number, date of birth, and Medicare number were compromised in the Data Breach.

85. Shortly after and as a result of the Data Breach, Plaintiff Ronne was the victim of fraud and identity theft. Specifically, she experienced a large increase in spam and suspicious phone calls, texts, and emails, such as letters allegedly from the State of North Dakota and from GeekSquad saying Plaintiff Ronne owes money. As a result, Plaintiff Ronne no longer answers

calls from phone numbers she does not recognize. In addition, Plaintiff Ronne has had unauthorized purchases attempted with GeekSquad, which her bank is investigating, and $238 was taken out of her bank account.

86. As a result of the Data Breach and as recommended in the Notice, Plaintiff Ronne made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, closely reviewing financial statements, logging into online accounts to check activity, obtaining her credit report from the credit reporting agencies, closing and opening new bank accounts, maintaining credit monitoring, and continually monitoring her credit information. Plaintiff Ronne has spent significant time responding to the Data Breach and will continue to spend valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. Plaintiff Ronne suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced increased concerns regarding the loss of her privacy as well as anxiety over the impact of cybercriminals accessing and using her PII and PHI.

87. Plaintiff Ronne believed that Aetna would protect her PII and PHI once she provided it to Aetna. Plaintiff Ronne would not have enrolled with Aetna if she had known Aetna would not adequately protect her PII and PHI.

88. Thus, as a result of the Data Breach, Plaintiff Ronne has faced and continues to face a present and continuing risk of fraud and identity theft for her lifetime. Plaintiff Ronne has a continuing interest in ensuring that her PII and PHI, which upon information and belief remains backed up in Aetna's possession, is protected and safeguarded from future data breaches.

**Plaintiff Gordon Titcomb**

89. Plaintiff Gordon Titcomb ("Plaintiff Titcomb") is a citizen and resident of Connecticut.

90. Plaintiff Titcomb has maintained health insurance coverage through Aetna. Aetna required Plaintiff Titcomb to provide his PII and PHI to Aetna in order to receive health insurance benefits and other services from Aetna. Upon information and belief, Aetna provided Plaintiff Titcomb's PII and PHI to NationsBenefits after he enrolled with Aetna.

91. Plaintiff Titcomb received a letter dated April 27, 2023, notifying Plaintiff Titcomb that as a health plan holder of Aetna his first name, middle initial, last name, gender, health plan subscriber identification number, address, phone number, and date of birth were compromised in the Data Breach.

92. Shortly after and as a result of the Data Breach, Plaintiff Titcomb was the victim of fraud and identity theft. Specifically, he experienced a large increase in spam and suspicious phone calls, texts, and emails from strangers, including ones requesting his response and to press a number to respond. In addition, he has received bills for unauthorized charges, such as for computer help and computer updates.

93. As a result of the Data Breach and as recommended in the Notice, Plaintiff Titcomb made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to, researching the Data Breach, closely reviewing financial statements, logging into online accounts to check activity, and continually monitoring his credit information. Plaintiff Titcomb has spent significant time responding to the Data Breach and will continue to spend valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. Plaintiff Titcomb suffered lost time, annoyance, interference, and inconvenience as a result of the

Data Breach and has experienced increased concerns regarding the loss of his privacy and anxiety, including a fear of financial loss and fear of further privacy loss, over the impact of cybercriminals accessing and using her PII and PHI.

94. Plaintiff Titcomb believed that Aetna would protect his PII and PHI once he provided it to Aetna. Plaintiff Titcomb would not have enrolled with Aetna if he had known Aetna would not adequately protect her PII and PHI.

95. Thus, as a result of the Data Breach, Plaintiff Titcomb has faced and continues to face a present and continuing risk of fraud and identity theft for his lifetime. Plaintiff Titcomb has a continuing interest in ensuring that his PII and PHI, which upon information and belief remains backed up in Aetna's possession, is protected and safeguarded from future data breaches.

**Plaintiff Rodrick Veazey**

96. Plaintiff Rodrick Veazey ("Plaintiff Veazey") is a citizen and resident of Florida.

97. Plaintiff Veazey has maintained health insurance coverage through Aetna. Aetna required Plaintiff Veazey to provide his PII and PHI to Aetna in order to receive health insurance benefits and other services from Aetna. Upon information and belief, Aetna provided Plaintiff Veazey's PII and PHI to NationsBenefits after he enrolled with Aetna.

98. Plaintiff Veazey received a letter dated April 27, 2023, notifying Plaintiff Veazey that as a health plan holder of Aetna his first name, middle initial, last name, gender, health plan subscriber identification number, address, phone number, date of birth, and Medicare number were compromised in the Data Breach.

99. Shortly after and as a result of the Data Breach, Plaintiff Veazey was the victim of fraud. Specifically, he experienced a large increase in spam and suspicious phone calls, texts, and

emails from strangers trying to solicit a response and gain personal information. Indeed, Plaintiff Veazey was recently informed by his bank that his email address appeared on the dark web.

100. As a result of the Data Breach and as recommended in the Notice, Plaintiff Veazey made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to, researching the Data Breach, closely reviewing financial statements, logging into online accounts to check activity daily, and continually monitoring his credit information. Plaintiff Veazey has spent significant time responding to the Data Breach and will continue to spend valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. Plaintiff Veazey suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced increased concerns regarding the loss of her privacy as well as anxiety, including fear of identity theft, anger at repeated data breaches, and general anxiety over the impact of cybercriminals accessing and using her PII and PHI.

101. Plaintiff Veazey believed that Aetna would protect his PII and PHI once he provided it to Aetna. Plaintiff Veazey would not have enrolled with Aetna if he had known Aetna would not adequately protect his PII and PHI.

102. Thus, as a result of the Data Breach, Plaintiff Veazey has faced and continues to face a present and continuing risk of fraud and identity theft for his lifetime. Plaintiff Veazey has a continuing interest in ensuring that his PII and PHI, which upon information and belief remains backed up in Aetna's possession, is protected and safeguarded from future data breaches.

**Plaintiff Nicholas Venezia**

103. Plaintiff Nicholas Venezia ("Plaintiff N. Venezia") is a citizen and resident of New York.

104. Plaintiff N. Venezia has maintained health insurance coverage through Aetna. Aetna required Plaintiff N. Venezia to provide his PII and PHI to Aetna in order to receive health insurance benefits and other services from Aetna. Upon information and belief, Aetna provided Plaintiff N. Venezia's PII and PHI to NationsBenefits after he enrolled with Aetna.

105. Plaintiff N. Venezia received a letter dated April 27, 2023, notifying Plaintiff N. Venezia that as a health plan holder of Aetna his first name, last name, gender, health plan subscriber identification number, address, phone number, and date of birth were compromised in the Data Breach.

106. Shortly after and as a result of the Data Breach, Plaintiff N. Venezia was the victim of fraud. Specifically, Plaintiff N. Venezia has experienced an increase in spam phone calls.

107. As a result of the Data Breach and as recommended in the Notice, Plaintiff N. Venezia made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to, researching the Data Breach, calling Aetna and/or NationsBenefits, closing the credit card account that was opened in his wife's name, closely reviewing financial statements, logging into online accounts to check activity daily, obtaining credit reports, placing credit holds with credit monitors he already had, and continually monitoring his credit information. Plaintiff N. Venezia has spent significant time, approximately six hours initially in addition to the time spent daily, responding to the Data Breach and will continue to spend valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. Plaintiff N. Venezia suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced increased concerns regarding the loss of his privacy as well as anxiety, including fear of his information on the dark web, over the impact of cybercriminals accessing and using her PII and PHI.

108. Plaintiff N. Venezia believed that Aetna would protect his PII and PHI once he provided it to Aetna. Plaintiff N. Venezia would not have enrolled with Aetna if he had known Aetna would not adequately protect his PII and PHI.

109. Thus, as a result of the Data Breach, Plaintiff N. Venezia has faced and continues to face a present and continuing risk of fraud and identity theft for his lifetime. Plaintiff N. Venezia has a continuing interest in ensuring that his PII and PHI, which upon information and belief remains backed up in Aetna's possession, is protected and safeguarded from future data breaches.

**Plaintiff Valarie Venezia**

110. Plaintiff Valarie Venezia ("Plaintiff V. Venezia") is a citizen and resident of New York.

111. Plaintiff V. Venezia has maintained health insurance coverage through Aetna. Aetna required Plaintiff V. Venezia to provide her PII and PHI to Aetna in order to receive health insurance benefits and other services from Aetna. Upon information and belief, Aetna provided Plaintiff V. Venezia's PII and PHI to NationsBenefits after she enrolled with Aetna.

112. Plaintiff V. Venezia received a letter dated April 27, 2023, notifying Plaintiff V. Venezia that as a health plan holder of Aetna her first name, middle initial, last name, gender, health plan subscriber identification number, address, phone number, and date of birth were compromised in the Data Breach.

113. Shortly after and as a result of the Data Breach, Plaintiff V. Venezia was the victim of fraud and identity theft. Specifically, Plaintiff V. Venezia has received bills for charges that were not made by her and has experienced health insurance-related fraud since January 2023 as well as a credit card being opened in her name. Additionally, Plaintiff V. Venezia was recently informed that her confidential information is on the dark web.

114. As a result of the Data Breach and as recommended in the Notice, Plaintiff V. Venezia made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to, researching the Data Breach, calling Aetna and/or NationsBenefits to seek information about the breach, closely reviewing financial statements, logging into online accounts to check activity, obtaining her credit report from the credit reporting agencies, freezing her credit, signing up for credit monitoring – and paying for additional credit monitoring services – and continually monitoring her credit information. Plaintiff V. Venezia has spent significant time responding to the Data Breach and will continue to spend valuable time she otherwise would have spent on other activities, including but not limited to, work and/or recreation. Plaintiff V. Venezia suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced increased concerns regarding the loss of her privacy as well as anxiety, including a constant fear of further identity theft, over the impact of cybercriminals accessing and using her PII and PHI.

115. Plaintiff V. Venezia believed that Aetna would protect her PII and PHI once she provided it to Aetna. Plaintiff V. Venezia would not have enrolled with Aetna if she had known Aetna would not adequately protect her PII and PHI.

116. Thus, as a result of the Data Breach, Plaintiff V. Venezia has faced and continues to face a present and continuing risk of fraud and identity theft for her lifetime. Plaintiff V. Venezia has a continuing interest in ensuring that her PII and PHI, which upon information and belief remains backed up in Aetna's possession, is protected and safeguarded from future data breaches.

**Plaintiff Donna Vogel**

117. Plaintiff Donna Vogel ("Plaintiff D. Vogel") is a citizen and resident of Ohio.

118. Plaintiff D. Vogel has maintained health insurance coverage through Aetna. Aetna required Plaintiff D. Vogel to provide her PII and PHI to Aetna in order to receive health insurance benefits and other services from Aetna. Upon information and belief, Aetna provided Plaintiff D. Vogel's PII and PHI to NationsBenefits after she enrolled with Aetna.

119. Plaintiff D. Vogel received a letter dated April 27, 2023, notifying Plaintiff D. Vogel that as a health plan holder of Aetna her first name, last name, gender, health plan subscriber identification number, address, phone number, date of birth, and Medicare number were compromised in the Data Breach.

120. Shortly after and as a result of the Data Breach, Plaintiff D. Vogel was the victim of fraud. Specifically, she experienced a large increase in spam and suspicious phone calls, texts, and emails from strangers asking her to respond or to press a number "to continue."

121. As a result of the Data Breach and as recommended in the Notice, Plaintiff D. Vogel made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to, researching the Data Breach, closely reviewing financial statements, logging into online accounts to check activity, and continually monitoring her credit information. Plaintiff D. Vogel has spent significant time, approximately one and a half hours each month, responding to the Data Breach and will continue to spend valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. Plaintiff D. Vogel suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach.

122. Plaintiff D. Vogel believed that Aetna would protect her PII and PHI once she provided it to Aetna. Plaintiff D. Vogel would not have enrolled with Aetna if she had known Aetna would not adequately protect her PII and PHI.

123. Thus, as a result of the Data Breach, Plaintiff D. Vogel has faced and continues to face a present and continuing risk of fraud and identity theft for her lifetime. Plaintiff D. Vogel has a continuing interest in ensuring that her PII and PHI, which upon information and belief remains backed up in Aetna's possession, is protected and safeguarded from future data breaches.

**Plaintiff John Vogel**

124. Plaintiff John Vogel ("Plaintiff J. Vogel") is a citizen and resident of Ohio.

125. Plaintiff J. Vogel has maintained health insurance coverage through Aetna. Aetna required Plaintiff J. Vogel to provide his PII and PHI to Aetna in order to receive health insurance benefits and other services from Aetna. Upon information and belief, Aetna provided Plaintiff J. Vogel's PII and PHI to NationsBenefits after he enrolled with Aetna.

126. Plaintiff J. Vogel received a letter dated April 27, 2023, notifying Plaintiff J. Vogel that as a health plan holder of Aetna his first name, last name, gender, health plan subscriber identification number, address, phone number, date of birth, and Medicare number were compromised in the Data Breach.

127. Shortly after and as a result of the Data Breach, Plaintiff J. Vogel was the victim of fraud. Specifically, he experienced a large increase in spam and suspicious phone calls, texts, and emails from strangers, including those asking him to press a number to continue or requesting a response.

128. As a result of the Data Breach and as recommended in the Notice, Plaintiff J. Vogel made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to, researching the Data Breach, closely reviewing financial statements, logging into online accounts to check activity, and continually monitoring his credit information. Plaintiff J. Vogel has spent significant time, approximately one and a half hours each month, responding to the Data Breach

and will continue to spend valuable time he otherwise would have spent on other activities, including but not limited to, work and/or recreation. Plaintiff J. Vogel suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach. Plaintiff J. Vogel is fearful and concerned someone might end up using his information to make large purchases or create fraudulent accounts as a result of the impact of cybercriminals accessing and using his PII and PHI.

129. Plaintiff J. Vogel believed that Aetna would protect his PII and PHI once he provided it to Aetna. Plaintiff J. Vogel would not have enrolled with Aetna if he had known Aetna would not adequately protect his PII and PHI.

130. Thus, as a result of the Data Breach, Plaintiff J. Vogel has faced and continues to face a present and continuing risk of fraud and identity theft for his lifetime. Plaintiff J. Vogel has a continuing interest in ensuring that his PII and PHI, which upon information and belief remains backed up in Aetna's possession, is protected and safeguarded from future data breaches.

131. Plaintiffs have taken reasonable steps to maintain the confidentiality of their PII and PHI, including but not limited to, protecting their usernames and passwords, using only strong passwords for their accounts, and refraining from browsing potentially unsafe websites.

132. Each Plaintiff suffered a concrete and particularized injury as a result of Aetna's failure to protect their PII and PHI and the subsequent disclosure of their PII and PHI to unauthorized parties without their consent.

**B. Defendants**

133. Defendant Aetna Inc. is a Pennsylvania corporation with its principal place of business located at 151 Farmington Ave., Hartford, Connecticut 06156.

134. Defendant Aetna Life Insurance Company is a Connecticut corporation with its principal place of business located at 151 Farmington Ave., Hartford, Connecticut 06156 and is a wholly owned subsidiary of Aetna Inc.

## FACTUAL ALLEGATIONS

### A. Aetna's Data Protection Obligations

135. Aetna is a leading provider of health insurance services in the United States. Aetna offers a range of healthcare products and services to employers, individuals, college students, and part-time and hourly workers nationwide.

136. Aetna's health insurance offerings include medical, pharmacy, dental, behavioral health, group life, and disability plans, and several Medicare offerings, including Medicare Advantage.

137. Aetna's Medicare Advantage plans are an alternative to Medicare Parts A and B, and often incorporate prescription drug coverage (Part D), as well as additional benefits not covered by Medicare such as vision, hearing, and dental care.

138. Aetna also offers Medicare Supplement Insurance, or "Medigap" plans, which help cover some of the healthcare costs that Medicare does not pay, standalone prescription drug (Part D) plans, and a combination plan called the Aetna Dual Eligible Special Needs Plan ("D-SNP") for those eligible for both Medicare and Medicaid.

139. As part of its Medicare plan offerings, Aetna partners with NationsBenefits to provide certain benefits to Aetna health plan holders such as Plaintiffs and Class Members.

140. Individuals such as Plaintiffs and Class Members who enroll with Aetna are required, by Aetna, to provide sensitive PII and PHI to Aetna.

141. Aetna, through privacy policies, codes of conduct, company security practices, and other conduct, implicitly and explicitly promised to safeguard Plaintiffs' and Class Members' PII and PHI.

142. Aetna's Notice of Privacy Practices ("Privacy Policy") states that it collects PII and PHI from Plaintiffs and Class Members relating to an individual's "health, medical conditions, prescriptions, and payment for health care products or services," such as demographic data, health details, test results, insurance information, and other information used to identify an individual or that is linked to an individual's health care or health care coverage.[5]

143. Aetna and its affiliates have a non-delegable duty under federal law to ensure that all health plan holder information it collects and stores is secure, and that any vendors or business associates with whom it shares information with also maintain adequate and commercially reasonable data security practices to ensure the protection of health plan holders' PII and PHI.

144. Indeed, Aetna's entire business depends on health plan holders entrusting it with their PII and PHI. Without health plan holders' PII and PHI, Aetna would not be able to provide health insurance benefits and other services and certainly would not be able to bill health plan holders and collect payment for health insurance benefits and other services rendered. More specifically, to provide health insurance benefits, Aetna knows that its health plan holders must trust that Aetna is keeping their PII and PHI private and secure. If Aetna's health plan holders lack trust in Aetna or knew Aetna would insecurely store, safeguard, or transmit their PII and PHI, then they will not disclose that information to it and would choose a competitor for health insurance benefits and other services.

---

[5] *Medicare Notice of Privacy Practices*, AETNA, https://www.aetnamedicare.com/content/dam/aetna/pdfs/wwwaetnamedicarecomSSL/individual/2022/member/Notice_of_Privacy_Policies.pdf (last accessed on Sept. 18, 2023).

145. This is why Aetna is a covered entity under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), *see* 45 C.F.R. §160.102, and as such is required to comply with the HIPAA Privacy Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

146. These rules establish national standards for the protection of patient information, including protected health information, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. *See* 45 C.F.R. §160.103.

147. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."

148. HIPAA requires that Aetna implement appropriate safeguards for this information.

149. HIPAA mandates that a covered entity, such as Aetna, may disclose PHI to a "business associate," only if the covered entity obtains satisfactory assurances that the business associate will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and assist in compliance with HIPAA privacy obligations. *See* 45 CFR §§164.502(e), 164.504(e), 164.532(d) and (e).

150. HIPAA also requires that Aetna provide every health plan holder, such as Plaintiffs and Class Members, with a privacy notice.

151. Aetna's privacy notice, as set forth in its Privacy Policy, informs health plan holders of, among other things, how Aetna uses and shares PII and PHI collected from its health plan

holders, health plan holders' rights under the law, and how Aetna complies with law and safeguards health plan holders' information.

152. As to health plan holders' legal rights, Aetna advises that "[u]nder federal privacy laws" health plan holders have the right to "[b]e notified after a breach of [their] PHI."[6]

153. Specifically, HIPAA requires that Aetna provide notice of a breach of unsecured protected health information, which includes protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons – *i.e.*, non-encrypted data.

154. Further, Aetna's Privacy Policy assures members that it keeps the information that it and its affiliates or subsidiaries collect and store – especially PHI – safe:

> We use administrative, technical and physical safeguards to keep your information from unauthorized access and other threats and hazards to its security and integrity. We comply with all state and federal laws that apply related to the security and confidentiality of your PHI. We don't destroy your PHI even when you end your coverage with us. We may need to use and share it even after your coverage terminates. (We describe the reasons for using or sharing in this Notice.) We will continue to protect your information against inappropriate use or disclosure.[7]

155. Aetna's Privacy Policy acknowledges that "[f]ederal privacy law requires us to keep your PHI private. And we must tell you about our legal duties and privacy practices. We must also follow the terms of the Notice in effect."[8]

156. Further, Aetna outlines "17 steps for securing health information" and states, "We aim beyond the industry standard." Aetna specifically states that one of the key steps it takes to safeguard member data is to "[a]ssess our vendors and how they protect our data."[9]

---

6 *Id*.

7 *Id*.

8 *Id.*; *see also Notice of Privacy Practices*, AETNA (Aug. 2022), https://www.aetna.com/document-library/legal-notices/documents/health-notice-of-privacy-practices.pdf.

9 *17 steps for securing health information*, AETNA, https://www.aetna.com/document-library/about-aetna-insurance/document-library/17-steps-securing-health-information.pdf (last accessed on Sept. 18, 2023).

157. Aetna, however, failed to adhere to its legal duties to protect Plaintiffs' and Class Members' PII and PHI.

### B. Aetna Collects Health Plan Holders' PII and PHI for Its Own Commercial, Financial Benefit

158. Aetna outsources several benefits and services its health plan holders are entitled to third-party vendor providers rather than provide those benefits to Aetna health plan holders itself. One such third-party vendor provider that Aetna sourced the provision of benefits to is NationsBenefits.

159. Aetna derives financial benefit from its partnership with NationsBenefits. According to NationsBenefits, for health plans such as Aetna, "[p]artnering with a leading supplemental benefits administrator, such as NationsBenefits, is a key component for successfully… [r]educing [c]osts" as well as "[e]nabling [g]rowth and [r]etention."[10]

160. NationsBenefits describes itself as "a leading provider of supplemental benefits, flex cards, and member engagement solutions that partners with managed care organizations to provide innovative healthcare solutions designed to drive growth, improve outcomes, reduce costs, and delight members."[11]

161. NationsBenefits provides these services through a "comprehensive suite of innovative supplemental benefits, payments platform, and member engagement solutions [which] help health plans deliver high quality benefits to their members that help address social determinants of health and improve member health outcomes and satisfaction."[12]

---

[10] *Why Choose NationsBenefits?*, NATIONSBENEFITS, https://www.nationsbenefits.com/health-plans (last accessed on Sept. 18, 2023).

[11] *About Us*, NATIONSBENEFITS, https://www.nationsbenefits.com/about-us (last accessed on Sept. 18, 2023).

[12] *Id*.

162. In doing so, Aetna provided the PII and PHI of millions of Aetna customers to NationsBenefits without adequately reviewing and evaluating NationsBenefits' information technology security and systems.

163. Worse, it appears that Aetna provided the information of millions of Aetna customers to NationsBenefits ***before*** Aetna's health plan holders attempted to use the programs offered by NationsBenefits, resulting in Aetna sharing the PII and PHI of millions of Aetna health plan holders who never interacted with NationsBenefits at all.

164. As such, Aetna affirmatively disclosed Plaintiffs' and Class Members' PII and PHI to NationsBenefits without consent, without any legitimate business need to do so, and when NationsBenefits was not authorized to receive the information.

165. Even assuming Aetna had a legitimate business reason to disclose PII and PHI to NationsBenefits before any member desired to use its services, Aetna had duties to ensure that each of its third-party vendors, including NationsBenefits, adopted reasonable measures to protect the PII and PHI of Plaintiffs and Class Members from involuntary disclosure to third parties.

166. Therefore, Plaintiffs and Class Members reasonably relied on Aetna to adequately review and evaluate the information technology security systems of vendors, such as NationsBenefits, and to ensure that their PII and PHI provided to the vendors chosen by Aetna would remain confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

### C. The Data Breach Is Announced

167. To provide the services outlined above and others, NationsBenefits used the GoAnywhere MFT software provided by third-party vendor Fortra, LLC ("Fortra") to exchange files with Aetna containing the PII and PHI of Plaintiffs and Class Members.

168. Upon information and belief, Aetna has sufficient control over Fortra's file transfer platform, GoAnywhere, to properly secure and encrypt Plaintiffs' and Class Members' PII and PHI that it exchanged with NationsBenefits over the GoAnywhere platform.

169. Unfortunately for Plaintiffs and Class Members, the Data Breach occurred, when from January 30, 2023, through February 7, 2023, an unauthorized third-party hacker group exploited a vulnerability in the Fortra GoAnywhere MFT software and began accessing and exfiltrating Plaintiffs' and Class Members' PII and PHI, which previously had been exchanged between Aetna and NationsBenefits via the Fortra GoAnywhere MFT software.

170. NationsBenefits became aware of the Data Breach on February 7, 2023. NationsBenefits then notified Aetna of the Data Breach on February 9, 2023. Yet Plaintiffs and Class Members were not notified of the Data Breach until April 27, 2023, when *NationsBenefits* (not Aetna) mailed out notification letters to individuals whose information had been compromised. Most individuals did not receive the letters until early May. This nearly three-month delay deprived Plaintiffs and Class Members of the ability to take steps to mitigate the damages caused by the Data Breach.

171. Below are relevant excerpts from the letters sent to Aetna health plan holders whose information was compromised in the Data Breach ("Notice of Data Breach" or "Notice"):

> NationsBenefits Holding, LLC, and its affiliates and subsidiaries (collectively, "NationsBenefits" or "we"), provides benefits administration services to your health insurer, [client_name]. We place a high value on maintaining the privacy and security of the information we maintain for our health plan customers. Regrettably, this letter is to inform you that a vendor we used to exchange files with Aetna[13] was recently the victim of a cybersecurity attack, which impacted some of your personal information. We notified Aetna of this incident on February 9, 2023.

[13] Steve Alder, *NationsBenefits Holdings Confirms 3 Million Record Data Breac*h, THE HIPPA JOURNAL (May 8, 2023), https://www.hipaajournal.com/nationsbenefits-holdings-confirms-3-million-record-data-breach/; *see also Cases Currently Under Investigation*, *supra* note 4.

> This letter explains the incident, the measures we have taken in response and the steps you can take.
>
> What Happened? NationsBenefits used software provided by a third-party vendor, Fortra, LLC ("Fortra"), to securely exchange files with your health plan. On or around January 30, 2023, Fortra experienced a data security incident in which a malicious actor(s) accessed or acquired the data of multiple organizations, including NationsBenefits. When we learned of this incident on February 7, 2023, we immediately took steps to secure our systems and launched an investigation, which was conducted by an experienced outside law firm and a leading cybersecurity firm. As part of our investigation, NationsBenefits analyzed the impacted data to determine whether any individual's personal information was subject to unauthorized access or acquisition. On February 23, 2023, NationsBenefits confirmed that, unfortunately, some of your personal information was affected by the incident.[14]

172. Upon information and belief, the Notice of Data Breach was drafted and publicized under the direction and with the approval of Aetna.

173. NationsBenefits' filing with the U.S. Department of Health and Human Services ("HHS") and public reporting has revealed that the PII and PHI of "3,037,303 health plan members, including, but not limited to, Aetna Affiliated Covered Entities ("ACE")," was compromised in the Data Breach and that "[t]he compromised information included: first and last name, address, phone number, date of birth, gender, health plan subscriber ID number, Social Security number, and/or Medicare number."[15]

174. NationsBenefits' filing with the Office of the Maine Attorney General has further confirmed that the PII and PHI compromised in the Data Breach includes names and other personal identifiers "in combination with" Social Security Number(s).[16]

---

[14] Letter from Glenn M. Parker MD, NationsBenefits Holdings, LLC to Aetna Clients, https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-187.pdf (last accessed on Sept. 18, 2023).

[15] Alder, *supra* note 13.

[16] *Data Breach Notifications, NationsBenefits Holdings, LLC, supra* note 1.

175. The Notice recommended that Plaintiffs and Class Members "remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity" and to follow the below steps to further protect themselves:

a. order your free credit report;

b. if you believe you are the victim of identity theft or have reason to believe your personal information has been misused, contact the FTC and/or your state's attorney general office about for information on how to prevent or avoid identity theft;

c. place a security freeze; and

d. place a fraud alert.[17]

176. Aetna thus largely placed the burden on Plaintiffs and Class Members to take measures to protect themselves.

177. Aetna also offered credit monitoring services to some Class Members for a period of 24 months. Such measures, however, are insufficient to protect Plaintiffs and Class Members from the lifetime risks they each now face. As another element of damages, Plaintiffs and Class Members seek a sum of money sufficient to provide Plaintiffs and Class Members identity theft protection services for their respective lifetimes.

178. Aetna had a non-delegable duty to ensure that its systems and those of its vendors and business associates, including NationsBenefits, were sufficient to adequately secure Aetna health plan holders' PII and PHI. By failing to adequately monitor and audit the data security systems of NationsBenefits, Aetna put members' PII and PHI at severe risk.

[17] Letter from Glenn M. Parker MD, *supra* note 14.

179. As evidenced by the Notice of Data Breach, Aetna failed to:

a. properly secure and encrypt Plaintiffs' and Class Members' PII and PHI that Aetna exchanged with NationsBenefits over the GoAnywhere platform;[18]

b. ensure that its direct and indirect technology partners and business associates ensured the proper encryption of Plaintiffs' and Class Members' PII and PHI;[19]

c. properly select and supervise its technology partners and business associates and ensure their compliance with information security best practices;[20]

d. ensure that its direct and indirect technology partners and business associates properly monitored and logged the ingress and egress of network traffic involving Plaintiffs' and Class Members' sensitive data;[21] and

e. ensure that its direct and indirect technology partners and business associates implemented sufficient processes to quickly detect and respond to data breaches, security incidents, or intrusions.[22]

**D. Aetna Failed to Provide Proper Notice of the Data Breach**

180. As detailed above, Aetna has never directly notified Aetna health plan holders that their information has been compromised in the Data Breach. Moreover, while NationsBenefits has stated it learned of the Data Breach on February 7, 2023, NationsBenefits failed to even begin notifying Plaintiffs and Class Members until April 27, 2023, via U.S. Mail.

181. Aetna appears to have disavowed any duty to notify its health plan holders of the Data Breach, and instead deferred to NationsBenefits' decision to choose to notify individuals only

[18] *Id.* ("NationsBenefits confirmed that, unfortunately, some of your personal information was affected by the incident.").

[19] *Id.*

[20] *Id.*

[21] *Id.* ("On or around January 30, 2023, Fortra experienced a data security incident in which a malicious actor(s) accessed or acquired the data of multiple organizations, including NationsBenefits," but NationsBenefits did not "learn[] of this incident [until] February 7, 2023.").

[22] *Id.*

via U.S. mail, even though both Aetna and NationsBenefits possess telephone and email contact information for each customer, which is likely more effective at reaching those individuals than U.S. mail.

182. Additionally, the three-month delay – a facially unreasonable amount of time under any measure – prevented Plaintiffs and Class Members from taking steps to mitigate the damage caused by the Data Breach.

183. Instead, and to protect its own financial interests, Aetna concealed the Data Breach for almost three months, allowing the unauthorized third party to potentially exploit Plaintiffs' and Class Members' PII and PHI without any mitigation steps being taken. Aetna did this despite knowing that the information was in possession of bad actors looking to exploit the PII and PHI for profit, a fact Aetna knew shortly after discovery of the Data Breach.

184. Plaintiffs and Class Members were thus deprived of the opportunity to take any steps to prevent damage by Aetna's concealment of the Data Breach and failure to provide timely and adequate notice of the Data Breach to Plaintiffs and Class Members.

### E. Aetna Failed to Exercise Due Care in Compliance with FTC Guidance and Industry Standards

185. Federal and state governments have established security standards and issued recommendations to reduce the number and size of data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for businesses, highlighting the importance of reasonable data and cyber security practices. According to the FTC, the need for data and cyber security should be factored into all business decision-making.[23]

[23] *Start with Security: A Guide for Business* at 2, FTC (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

186. Aetna is prohibited by the Federal Trade Commission Act, 15 U.S.C. §45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

187. In 2016, the FTC updated its publication, *Protecting Private Information: A Guide for Business*, which established guidelines for fundamental data and cyber security principles and practices for business.[24] The guidelines note businesses should protect the personal customer and consumer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.[25] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[26]

188. The FTC recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and (most pertinent here) verify, monitory, and audit that third-party service providers have implemented reasonable security measures.

189. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and

---

[24] *Protecting Private Information: A Guide for Business*, FTC (Oct. 2016), https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business [https://perma.cc/9945-U4HV].

[25] *Id*.

[26] *Id*.

appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

190. These FTC enforcement actions include actions against healthcare providers and partners like Aetna. *See, e.g., In the Matter of LabMD, Inc., A Corp*, No. 9357, 2016 WL 4128215, at *32 (F.T.C. July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

191. Aetna's failure to employ reasonable and appropriate measures to protect against unauthorized access to members' PII and PHI, specifically by failing to verify, monitor, and audit that third-party service providers have implemented reasonable security measures, constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

192. Aetna also has obligations created by other federal and state laws and regulations, contracts, industry standards, and common law to maintain reasonable and appropriate physical, administrative, and technical measures to keep Plaintiffs' and Class Members' PII and PHI confidential and to protect it from unauthorized access and disclosure.

193. Given the magnitude of the risk and repercussions of a data breach or attack targeting this type of data, the likelihood of a data breach or attack, and Aetna's explicit awareness of these vulnerabilities, Aetna should have taken every reasonable precaution in developing a robust security program and protecting Plaintiffs' and the Class Members' PII and PHI.

194. Yet, despite its duties, representations, and promises, Aetna failed to adequately secure and protect their customers' data, allowing the Plaintiffs' and Class Members' PII and PHI to be accessed, disclosed, and misused.

195. Aetna also owed a duty to comply with industry standards in safeguarding PII and PHI, which – as discussed herein – it did not do.

196. Cyberattacks have become so notorious that the FBI and Secret Service issued an unprecedented warning in 2019 to potential targets so they were aware of, and prepared for, a potential attack.[27]

197. The U.S. government, various U.S. and international law enforcement agencies, cybersecurity industry groups and laboratories, and numerous industry trade groups have issued warnings and guidance on managing and mitigating phishing and ransomware threats. There are industry best practices for cybersecurity related to phishing and ransomware, some of which are particularly effective.

198. For example, in 2019, both Microsoft and Google publicly reported that using multi-factor authentication ("MFA") blocks more than 99% of automated hacks, including most ransomware attacks that occur because of unauthorized account access. Likewise, the reputable SANS Software Security Institute issued a paper stating "[t]ime to implement multi-factor authentication!"[28] An example of MFA implementation is receiving a text with a code when you input your username and password into a website; even if a cybercriminal knew your username and password, the cybercriminal would not be able to see the code on your phone and would thus be blocked from accessing your online account.

---

[27] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

[28] Matt Bromiley, *Bye Passwords: New Ways to Authenticate* at 3, SANS Software Security Inst. (July 2019), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE3y9UJ [https://perma.cc/ZSW9-QUEW].

199. In this regard, implementing MFA "can block over 99.9 percent of account compromise attacks."[29]

200. Because of the value of PII and PHI to hackers and identity thieves, companies in the business of obtaining, storing, maintaining, and securing PII and PHI, such as Aetna, have been identified as being particularly vulnerable to cyber-attacks. Cybersecurity firms have promulgated a series of best practices that, at minimum, should be implemented by sector participants including, but not limited to: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.[30]

201. Other best practices have been identified that, at a minimum, should be implemented by healthcare providers like Aetna, including but not limited to, educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

202. Yet, instead of following these widely adopted industry standards, Aetna failed to adequately secure and protect its health plan holders' data, allowing the Plaintiffs' and Class Members' PII and PHI to be accessed, disclosed, and misused by failing to verify, monitor, and

---

[29] *What Is Multi-Factor Authentication (MFA)?*, CONSENSUS TECHS., (Sept. 16, 2020), https://www.concensus.com/what-is-multi-factor-authentication/#:~:text=The%20proof%20that%20MFA%20works,percent%20of%20account%20compromise%20attacks [https://perma.cc/RKT2-LX5Z].

[30] *See Addressing BPO Information Security: A Three-Front Approach*, DATAMARK, Inc. (Nov. 2016), [https://web.archive.org/web/20211219185808/https://insights.datamark.net/addressing-bpo-information-security/] [https://perma.cc/NY6X-TFUY].

audit that third-party vendors and business associates, such as NationsBenefits, have implemented reasonable security measures.

### F. Aetna Violated HIPAA's Requirements to Safeguard Data and Regulatory Mandates

203. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.[31]

204. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII and PHI is properly maintained.[32]

205. Aetna is a covered entity pursuant to HIPAA. *See* 45 C.F.R. §160.102. Aetna must therefore comply with the HIPAA Privacy Rule and Security Rule. *See* 45 C.F.R. Part 160 and Part 164, Subparts A through E.

206. Aetna also is a covered entity pursuant to the Health Information Technology Act ("HITECH").[33] *See* 42 U.S.C. §17921, 45 C.F.R. §160.103.

207. The HIPAA and HITECH rules work in conjunction with the already established state laws relating to privacy. HIPAA and HITECH provide the guidelines for the standard of procedure dictating how patient medical information should be kept private.

---

[31] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

[32] *See* 45 C.F.R. §164.306 (security standards and general rules); 45 C.F.R. §164.308 (administrative safeguards); 45 C.F.R. §164.310 (physical safeguards); 45 C.F.R. §164.312 (technical safeguards).

[33] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

208. HIPAA's Privacy Rule, otherwise known as "Standards for Privacy of Individually Identifiable Health Information," establishes national standards for the protection of health information.

209. HIPAA's Security Rule, otherwise known as "Security Standards for the Protection of Electronic Protected Health Information," establishes national security standards for the protection of health information that is held or transferred in electronic form. *See* 42 C.F.R. §§ 164.302-164.318.

210. HIPAA limits the permissible uses of "protected health information" and prohibits the unauthorized disclosure of "protected health information." 45 C.F.R. §164.502. HIPAA requires that covered entities implement appropriate administrative, technical, and physical safeguards for this information and requires that covered entities reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart. *See* 45 C.F.R. §164.530(c).

211. HIPAA requires a covered entity or business associate to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. §164.530(e).

212. HIPAA requires a covered entity or business associate to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. §164.530(f).

213. Should a covered entity or business associate experience an unauthorized disclosure, it is required to conduct a Four Factor Risk Assessment (HIPAA Omnibus Rule). This standard requires that a covered entity or business associate must now undertake a four-factor risk assessment to determine whether or not PHI has been compromised and overcome the presumption that the breach must be reported. The four-factor risk assessment focuses on: (1) the nature and extent of the PHI involved in the incident (*e.g.*, whether the incident involved sensitive information like social security numbers or infectious disease test results); (2) the recipient of the PHI; (3) whether the PHI was actually acquired or viewed; and (4) the extent to which the risk that the PHI was compromised has been mitigated following unauthorized disclosure (*e.g.*, whether it was immediately sequestered and destroyed).[34]

214. The Data Breach itself resulted from a combination of inadequacies showing Aetna failed to comply with safeguards mandated by HIPAA. Aetna's security failures include, but are not limited to:

a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains, and transmits in violation of 45 C.F.R. §164.306(a)(1);

b. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. §164.312(a)(1);

c. Failing to implement adequate procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports, in violation of 45 C.F.R. §164.308(a)(1);

d. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. §164.308(a)(1);

[34] *See* 45 C.F.R. §164.402(2).

e. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. §164.306(a)(2);

f. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. §164.306(a)(3);

g. Failing to implement safeguards to ensure that Aetna's business associates adequately protect PHI;

h. Failing to ensure compliance with HIPAA security standards by Aetna's workforce in violation of 45 C.F.R. §164.306(a)(4);

i. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. §164.308(a)(6)(ii);

j. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. §164.530(b) and 45 C.F.R. §164.308(a)(5); and

k. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. §164.530(c).

215. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrates Aetna failed to comply with safeguards mandated by HIPAA regulations.

**G. Aetna's Members' PII and PHI Is Highly Valuable**

216. Aetna knew or should have known, because the protected PII and PHI that it acquires, stores, and utilizes is highly sensitive and of significant value to the owners of the PII and PHI and those who would use it for wrongful purposes, that Aetna would be a target of cybercriminals and that Plaintiffs and Class Members were the foreseeable victims of Aetna's wrongful conduct.

217. The healthcare industry in particular has experienced a large number of high-profile cyberattacks even in just the short period preceding the filing of this Complaint, and cyberattacks,

generally, have become increasingly more common. More healthcare data breaches were reported in 2020 than in any other year, showing a 25% increase.[35] Additionally, according to the HIPAA Journal, the largest healthcare data breaches have been reported beginning in April 2021.[36]

218. In the context of data breaches, healthcare is "by far the most affected industry sector."[37] Further, cybersecurity breaches in the healthcare industry are particularly devastating, given the frequency of such breaches and the fact that healthcare providers maintain highly sensitive and detailed PII.[38] And according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[39]

219. Despite the prevalence of public announcements of data breaches and data security compromises, Aetna failed to take appropriate steps to protect Plaintiffs' and Class Members' PII and PHI from being compromised.

**1. The Value of PII and PHI**

220. Personal information, such as PII and PHI, is property with inherent and sizeable market value. Its value is axiomatic, considering the market value and profitability of "Big Data" corporations in America. Alphabet Inc., the parent company of Google, aptly illustrated this in its 2020 Annual Report, when it reported a total annual revenue of $182.5 billion and net income of

---

35 *2020 Healthcare Data Breach Report*, HIPAA JOURNAL (Jan. 19, 2021) https://www.hipaajournal.com/2020-healthcare-data-breach-report/.

36 *April 2021 Healthcare Data Breach Report*, HIPAA JOURNAL (May 18, 2021) https://www.hipaajournal.com/april-2021-healthcare-data-breach-report/.

37 Rody Quinlan, *Healthcare Security: Ransomware Plays a Prominent Role in Covid-19 Era Breaches*, TENABLE (Mar. 10, 2021), https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches.

38 *See id.*

39 *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack*, SECURITY MAGAZINE (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack.

$40.2 billion.[40] Of this revenue, $160.7 billion was derived from its Google business, which is driven almost exclusively by leveraging the PII and PHI it collects about the users of its various free products and services. America's largest corporations profit almost exclusively through the use of PII and PHI, illustrating the considerable market value of PII and PHI.

221. Criminal law also recognizes the value of PII and PHI and the serious nature of the theft of such an asset by imposing prison sentences. This strong deterrence is necessary because cybercriminals earn significant revenue through stealing PII and PHI. Once a cybercriminal has unlawfully acquired personal data, the criminal can demand a ransom or blackmail payment for its destruction, use the information to commit fraud or identity theft, or sell the PII and PHI to another cybercriminal on a thriving black market.

222. Furthermore, personal information, such as PII and PHI, is a valuable commodity to identity thieves, particularly when such data is aggregated in large numbers. Former United States Attorney General William P. Barr made clear that consumers' sensitive personal information commonly stolen in data breaches "has economic value." The purpose of stealing large caches of personal data is to use it to defraud individuals or to place it for illegal sale and to profit from other criminals who buy the data and use it to commit fraud and identity theft. Indeed, cybercriminals routinely post stolen personal information for sale on anonymous websites, making the information widely available to a criminal underworld.

223. There is an active and robust market for this information. As John Sancenito, president of Information Network Associates, a company which helps other companies with recovery after data breaches, explained after a data breach "[m]ost of the time what [data breach

[40] Alphabet Inc., Annual Report (Form 10-K) at 32 (Feb. 3, 2021), https://www.sec.gov/ix?doc=/Archives/edgar/data/0001652044/000165204421000010/goog-20201231.htm.

hackers] do is they steal the data and then they sell the data on the dark web to the people who actually commit the fraud."[41]

224. Thus, Plaintiffs and Class Members rightfully place a high value not only on their PII and PHI, but also on the privacy of that data.

225. Once stolen, PII and PHI can be used in a number of different ways. One of the most common is that it is offered for sale on the "dark web," a heavily encrypted part of the Internet that makes it difficult for authorities to detect the location or owners of a website. The dark web is not indexed by normal search engines such as Google and is only accessible using a Tor browser (or similar tool), which aims to conceal users' identities and online activity. The dark web is notorious for hosting marketplaces selling illegal items, such as weapons, drugs, and PII and PHI. Websites appear and disappear quickly, making it a dynamic environment.

226. The forms of PII and PHI involved in this Data Breach are particularly concerning. Unlike credit or debit card numbers in a payment card data breach – which can quickly be frozen and reissued in the aftermath of a breach – unique Medicare ID numbers, health plan ID numbers, and Social Security numbers cannot be easily replaced. Even when such numbers are replaced, the process of doing so results in a major inconvenience to the subject person, requiring a wholesale review of the person's relationships with government agencies and any number of private companies to update the person's accounts with those entities.

227. Another example of criminals using PII and PHI for profit is the development of "Fullz" packages.[42]

---

[41] Priscilla Liguori, *Legislator, security expert weigh in on Rutter's data breach*, ABC27 (Feb. 14, 2020; updated Feb. 17, 2020), https://www.abc27.com/local-news/york/legislator-security-expert-weigh-in-on-rutters-data-breach/.

[42] "Fullz" is fraudster-speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the

228. Cyber-criminals can cross-reference two sources of PII and PHI to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

229. The development of "Fullz" packages means that stolen PII and PHI from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII and PHI stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs' and Class Members' stolen PII and PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

### 2. Data Breaches Put Consumers at Increased Risk of Fraud and Identity Theft

230. Cyberattacks and data breaches of health services companies are especially problematic because of the potentially permanent disruption they cause to the daily lives of their

more information you have on a victim, the more money can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record or more on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records For Sale in Underground Stolen From Texas Life Insurance Firm*, KREBS ON SECURITY, (Sep. 18, 2014), https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm/.

customers. Stories of identity theft and fraud abound, with hundreds of millions of dollars lost by everyday consumers every year as a result of internet-based identity theft attacks.[43]

231. The U.S. Government Accountability Office ("GAO") released a report in 2007 regarding data breaches, finding that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[44]

232. The FTC recommends that identity theft victims take several steps to protect their personal health and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (and to consider an extended fraud alert that lasts for seven years if identity theft occurs), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[45]

233. Cybercriminals use stolen PII and PHI, such as Social Security numbers, for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

234. Identity thieves can also use Social Security numbers to obtain a driver's license or other official identification card in the victim's name, but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, seek

---

[43] Albert Khoury, *Scam alert: 5 most costly data breaches (plus 5 states most targeted)*, KIM KIMANDO (July 27, 2022), https://www.komando.com/security-privacy/most-costly-data-breaches/847800/.

[44] *PII and PHI: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* ("GAO Report") at 2, GAO (June 2007), https://www.gao.gov/assets/270/262899.pdf [https://perma.cc/GCA5-WYA5].

[45] *Identity Theft Recovery Steps*, FTC, https://www.identitytheft.gov/#/Steps (last accessed on Sept. 18, 2021) [https://perma.cc/ME45-5N3A].

unemployment or other benefits, and may even give the victim's PII and PHI to police during an arrest, resulting in an arrest warrant being issued in the victim's name.

235. A study by the Identity Theft Resource Center ("ITRC") found that 96.7% of identity theft victims experienced costs and/or other harms from the criminal activity.[46] This includes devastating results, such as "I lost my home/place of residence" and "I couldn't care for my family." Moreover, the harms of identity theft are not limited to the affected individual and may adversely impact other associated persons and support systems, including government assistance programs. In the ITRC study, nearly one third of survey respondents had to request government assistance as a result of the identity theft, such as welfare, EBT, food stamps, or similar support systems.[47] The ITRC study concludes that "identity theft victimization has an extreme and adverse effect on each individual as well as all of the support systems and people associated with the individual."[48]

236. The PII and PHI exfiltrated in the Data Breach can also be used to commit identity theft by placing Plaintiffs and Class Members at a higher risk of "phishing," "vishing," "smishing," and "pharming,"[49] which are other ways for cybercriminals to exploit information they already have in order to get even more personally identifying information from a person through

---

[46] Jason Steele, *Credit Card and ID Theft Statistics*, CREDITCARDS.COM (updated Oct. 24, 2017), https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php [https://web.archive.org/web/20171215215318/https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php].

[47] *Id*.

[48] *Id*.

[49] Phishing is the fraudulent practice of sending emails or other messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers; Vishing is the fraudulent practice of making phone calls or leaving voice messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as bank details and credit card numbers; Smishing is the fraudulent practice of sending text messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords or credit card numbers; and Pharming is the fraudulent practice of directing internet users to a bogus website that mimics the appearance of a legitimate one, in order to obtain personal information such as passwords, account numbers, etc.

unsolicited email, text messages, and telephone calls purportedly from a legitimate company requesting personal, financial, and/or login credentials.

237. PII and PHI are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the cyber black market for years.

238. It must also be noted there may be a substantial time lag – measured in years – between when harm occurs and when it is discovered, and between when PII and PHI and/or financial information is stolen and when it is used. According to the GAO, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[50]

239. Furthermore, data breaches that expose any personal data, and in particular non-public data of any kind (*e.g.*, donation history or hospital records), directly and materially increase the chance that a potential victim is targeted by a spear phishing attack in the future, and spear phishing results in a high rate of identity theft, fraud, and extortion.[51]

240. There is a strong probability that entire batches of stolen information from the Data Breach have yet to be made available on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future. Indeed, some of the Plaintiffs and many Class Members are in the very early stages of their lives – in their twenties

---

[50] GAO Report, *supra* note 44 at 29.

[51] Josh Fruhlinger, *What is spear phishing? Examples, tactics, and techniques*, CSO (Apr. 7, 2022), https://www.csoonline.com/article/566789/what-is-spear-phishing-examples-tactics-and-techniques.html.

and thirties. Thus, as the Notice advises, Plaintiffs must vigilantly monitor their financial accounts for many years to come.

241. Aetna is a highly sophisticated party that regularly handles sensitive PII and PHI and thus knew or should have known that it would be a target for cybercriminals and the Plaintiffs' and Class Members' were foreseeable victims of Aetna's wrongful conduct described herein. Yet it failed to establish and/or implement appropriate administrative, technical, and/or physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class Members' PII and PHI to protect against anticipated threats of intrusion of such information.

242. The ramifications of Aetna's failure to keep Plaintiffs' and Class Members' PII and PHI secure are long lasting and severe. To avoid detection, identity thieves often hold stolen data for months or years before using it. Also, the sale of stolen information on the "dark web" may take months or more to reach end-users, in part because the data is often sold in small batches as opposed to in bulk to a single buyer. Thus, Plaintiffs and Class Members must vigilantly monitor their financial accounts *ad infinitum*.

243. Thus, Aetna knew, or should have known, the importance of safeguarding the PII and PHI entrusted to it and of the foreseeable consequences if its systems were breached. Aetna failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

244. Thus, Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

### H. Aetna Caused Reasonably Foreseeable Harm to Plaintiffs and Class Members

245. Charged with handling highly sensitive PII and PHI, including healthcare information, financial information, and insurance information, Aetna knew or should have known

the importance of safeguarding the PII and PHI that was entrusted to it. Aetna also knew or should have known of the foreseeable consequences if its vendors' and business associates' data security systems were breached. This includes the significant costs that would be imposed on Aetna's health plan holders, like Plaintiffs and Class Members, as a result of a breach. Aetna nevertheless failed to take adequate cybersecurity measures to prevent the Data Breach from occurring.

246. Because of the highly sensitive and personal nature of the information Aetna acquire and store, Aetna knew or reasonably should have known that it stored protected PII and PHI and transmitted that data to vendors and business associates and must comply with healthcare industry standards related to data security and all federal and state laws protecting customers' and patients' PII and PHI and provide adequate notice to customers if their PII or PHI is disclosed without proper authorization.

247. By obtaining, collecting, receiving, storing, and/or transmitting Plaintiffs' and Class Members' PII and PHI, Aetna assumed legal and equitable duties and knew, or should have known, that it was thereafter responsible for protecting Plaintiffs' and Class Members' PII and PHI from unauthorized disclosure.

248. Aetna could have prevented or mitigated the effects of the Data Breach by better selecting and verifying, supervising, and auditing its vendors and business associates.

249. As a result of Aetna's deficient security and monitoring measures, Plaintiffs and Class Members have been harmed by the compromise of their sensitive personal information, which is currently for sale on the dark web and through private sale to other cyber criminals and/or being used by criminals for identify theft and other fraud-related crimes.

250. Plaintiffs and Class Members face a substantial and imminent risk of fraud and identity theft as their names have now been linked with their Social Security numbers, bank

account numbers, emails, phone numbers, and physical addresses as a result of the Data Breach. These specific types of information are associated with a high risk of fraud.

251. Plaintiffs and Class Members also suffered a "loss of value" of their sensitive personal information when it was stolen by hackers in the Data Breach. A robust market exists for stolen personal information. Hackers sell personal information on the dark web – an underground market for illicit activity, including the purchase of hacked personal information – at specific identifiable prices. This market serves to determine the loss of value to Plaintiffs and Class Members.

252. As discussed above, Plaintiffs' and Class Members' stolen personal information is a valuable commodity to identity thieves.

253. Identity thieves can also combine data stolen in the Data Breach with other information about Plaintiffs and Class Members gathered from underground sources, public sources, or even Plaintiffs' and Class Members' social media accounts. Thieves can use the combined data to send highly targeted phishing emails to Plaintiffs and Class Members to obtain more sensitive information. Thieves can use the combined data to commit potential crimes, including opening new financial accounts in Plaintiffs' and Class Members' names, taking out loans in Plaintiffs' and Class Members' names, using Plaintiffs' and Class Members' information to obtain government benefits, filing fraudulent tax returns using Plaintiffs' and Class Members' information, obtaining Social Security numbers in Plaintiffs' and Class Members' names but with another person's photograph, and giving false information to police during an arrest.

254. Plaintiffs and Class Members also suffered "benefit of the bargain" damages. Plaintiffs and Class Members overpaid for services that should have been – but were not – accompanied by adequate data security. Part of the premiums paid by Plaintiffs and Class

Members to Aetna was intended to be used to fund adequate data security, including verifying, monitoring, and auditing that its vendors and business associates maintained adequate security measures. Plaintiffs and Class Members did not get what they paid for.

255. Plaintiffs and Class Members have spent and will continue to spend substantial amounts of time monitoring their accounts for identity theft and fraud, the opening of fraudulent accounts, disputing fraudulent transactions, and reviewing their financial affairs more closely than they otherwise would have done but for the Data Breach.

256. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.6% of U.S.-based workers are compensated on an hourly basis, while the other 44.4% are salaried.[52]

257. According to the U.S. Bureau of Labor Statistics' 2018 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per week;[53] leisure time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable income.'"[54] Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

---

[52] *Characteristics of minimum wage workers, 2022*, U.S. BUREAU OF LABOR STATISTICS https://www.bls.gov/opub/reports/minimum-wage/2022/home.htm (last accessed Sept. 19, 2023); Economic News Release, Table B-3. Average hourly and weekly earnings of all employees on private nonfarm payrolls by industry sector, seasonally adjusted, U.S. BUREAU OF LABOR STATISTICS, https://www.bls.gov/news.release/empsit.t19.htm (last accessed Sept. 19. 2023) (finding that on average, for August 2023, private-sector workers make $1,163 per 40-hour work week.).

[53] Cory Stieg, *You're spending your free time wrong – here's what to do to be happier and more successful*, CNBC (Nov. 6, 2019), https://www.cnbc.com/2019/11/06/how-successful-people-spend-leisure-time-james-wallman.html.

[54] *Id*.

258. Plaintiffs and Class Members are now deprived of the choice as to how to spend their valuable free hours and seek renumeration for the loss of valuable time as another element of damages.

259. Plaintiffs and Class Members may also incur out of pocket costs for protective measures such as identity theft protection, credit monitoring fees, credit report fees, credit freeze fees, fees for replacement cards, and similar costs related to the Data Breach.

260. Class Members who experience actual identity theft and fraud will also be harmed by the inability to use their credit or debit cards when their accounts are suspended or otherwise rendered unusable due to fraudulent charges. To the extent Class Members are charged monthly/annual fees for their credit and/or debit accounts, they are left without the benefit of that bargain while they await receipt of their replacement cards. Class Members will be harmed further by the loss of rewards points or airline mileage that they cannot accrue while awaiting replacement cards. The inability to use payment cards may also result in missed payments on bills and loans, late charges and fees, and adverse effects on their credit, including decreased credit scores and adverse credit notations.

261. In the case of a data breach, merely reimbursing a consumer for a financial loss due to identity theft or fraud does not make that individual whole again. On the contrary, after conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems."[55]

[55] Erika Harrell. Ph.D and Lynn Langton Ph.D., *Victims of Identity Theft, 2012*, U.S. DEP'T OF JUST., BUREAU OF JUST. STATS. (Dec. 2013), https://bjs.ojp.gov/content/pub/pdf/vit12.pdf.

262. A victim whose personal information has been stolen or compromised may not see the full extent of identity theft or fraud until long after the initial breach. Additionally, a victim whose personal information has been stolen may not become aware of charges when they are nominal, as typical fraud-prevention algorithms may not capture such charges. Those charges may be repeated, over and over again, on a victim's account.

263. The risk of identity theft and fraud will persist for years. Identity thieves often hold stolen data for months or years before using it to avoid detection. Also, the sale of stolen information on the dark web may take months or more to reach end-users, in part because the data is often sold in small batches to various individuals rather than in bulk to a single buyer. Thus, Plaintiffs and Class Members must vigilantly monitor their financial accounts *ad infinitum*.

## CLASS ACTION ALLEGATIONS

264. Pursuant to Fed. R. Civ. P. 23(b)(2) and 23(b)(3), as applicable, and 23(c)(4), Plaintiffs seek certification of the following nationwide class (the "Class" or the "Nationwide Class") of similarly situated persons for the state common law claims and for a declaratory judgment and other equitable relief:

> All Aetna customers whose PII and/or PHI were compromised in the Data Breach.

265. Pursuant to Fed. R. Civ. P. 23(b)(2) and 23(b)(3), as applicable, and 23(c)(4), Plaintiffs seek certification of statewide subclasses in the alternative to nationwide certification for the state common law claims, a declaratory judgment and other equitable relief, and state statutory consumer protection claims on behalf of residents of Connecticut, Florida, Georgia, Illinois, Massachusetts, Michigan, Nevada, New York, North Dakota, Ohio, and Oklahoma (the "Subclasses"). Each Subclass is defined as follows:

> Connecticut Subclass: All Aetna customers residing in Connecticut whose PII and/or PHI was compromised in the Data Breach.

Florida Subclass: All Aetna customers residing in Florida whose PII and/or PHI was compromised in the Data Breach.

Georgia Subclass: All Aetna customers residing in Georgia whose PII and/or PHI was compromised in the Data Breach.

Illinois Subclass Members: All Aetna customers residing in Illinois whose PII and/or PHI was compromised in the Data Breach.

Massachusetts Subclass: All Aetna customers residing in Massachusetts whose PII and/or PHI was compromised in the Data Breach.

Michigan Subclass: All Aetna customers residing in Michigan whose PII and/or PHI was compromised in the Data Breach.

Nevada Subclass: All Aetna customers residing in Nevada whose PII and/or PHI was compromised in the Data Breach.

New York Subclass: All Aetna customers residing in New York whose PII and/or PHI was compromised in the Data Breach.

North Dakota Subclass: All Aetna customers residing in North Dakota whose PII and/or PHI was compromised in the Data Breach.

Ohio Subclass: All Aetna customers residing in Ohio whose PII and/or PHI was compromised in the Data Breach.

Oklahoma Subclass: All Aetna customers residing in Oklahoma whose PII and/or PHI was compromised in the Data Breach.

266. The Nationwide Class and Subclasses are collectively referred to as the Classes.

267. Excluded from the Classes are: (1) any judge or magistrate presiding over this action and members of their families; (2) Aetna and its subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which its parent has a controlling interest, and their respective current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Classes; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiffs' counsel and Aetna's counsel; (6) members of the jury; and (7) the legal representatives, successors, and assigns of any such excluded persons.

268. Plaintiffs reserve the right to amend or modify the Class and Subclass definitions with greater specificity after having had the opportunity to conduct discovery.

269. **Numerosity**. Consistent with Rule 23(a)(1), the members of the Classes are so numerous and geographically dispersed that the joinder is impractical. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the Class consists of the approximately 1,000,000 individuals whose PII and PHI were compromised as a result of the Data Breach. Those persons' names and addresses are available from Aetna's records, and Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include electronic mail, U.S. Mail, internet notice, and/or published notice. Upon information and belief, there are at least thousands of members in each Subclass, making joinder of all Subclass Members impractical.

270. **Commonality**. Rule 23(a)(2)'s commonality requirement is satisfied. There are many questions of law and fact common to each of the Classes. These common questions predominate over any individualized questions of individual Class and Subclass Members. These common questions of law and fact include, without limitation:

a. Whether Aetna owed a duty to Class and Subclass Members to safeguard their PII and PHI;

b. Whether Aetna failed to implement and maintain reasonable security procedures and monitoring practices appropriate for the nature and scope of the information compromised in the Data Breach;

c. Whether Aetna's conduct violated the FTC Act and/or HIPAA;

d. Whether Aetna's data security systems and monitoring processes prior to and during the Data Breach complied with applicable data security laws and regulations, including HIPAA and HITECH;

e. Whether Aetna's data security systems and monitoring processes prior to and during the Data Breach were consistent with industry standards;

f. Whether Aetna breached its duty to Class and Subclass Members to safeguard their PII and PHI;

g. Whether Aetna knew or should have known NationsBenefits' network and systems were susceptible to a data breach;

h. Whether Aetna knew or should have known that its data security procedures and monitoring processes were deficient;

i. Whether Aetna was negligent in failing to adequately monitor and audit the data security systems of its vendor / business associate NationsBenefits;

j. Whether Aetna's efforts (or lack thereof) to ensure the security of health plan holders' PII and PHI provided to vendors and business associates, such as NationsBenefits, were reasonable in light of known legal requirements.

k. Whether a contract existed between Class and Subclass Members and Aetna, providing that Aetna would implement and maintain reasonable security measures to protect and secure Class and Subclass Members' PII and PHI from unauthorized access and disclosure;

l. Whether Aetna breached contracts with Plaintiffs and Class and Subclass Members;

m. Whether Aetna was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiffs and Class and Subclass Members;

n. Whether Plaintiffs and Class Members maintained a confidential relationship with Aetna;

o. Whether Aetna knew or should have known Plaintiffs' and Class Members' PII and PHI was disclosed to Aetna in confidence;

p. Whether Aetna affirmatively disclosed Plaintiffs' and Class Members' PII and PHI to NationsBenefits without consent;

q. Whether Aetna engaged in unfair, unconscionable, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiffs and Class and Subclass Members;

r. Whether Aetna owed a duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class and Subclass Members;

s. Whether Aetna failed to notify Plaintiffs and Class and Subclass Members as soon as practicable and without delay after the Data Breach was discovered;

t. Whether Aetna's delay in informing Plaintiffs and Class and Subclass Members of the Data Breach was unreasonable;

u. Whether Aetna's method of informing Plaintiffs and Class and Subclass Members of the Data Breach was unreasonable;

v. Whether Aetna's conduct, including its failure to act, resulted in or was the proximate cause of the loss of the PII and PHI of Plaintiffs and Class and Subclass Members;

w. Whether Plaintiffs and Class and Subclass Members were injured and suffered damages or other losses because of Aetna's failure to reasonably protect their PII and PHI; and

x. Whether, as a result of Aetna's conduct, Plaintiffs and Class and Subclass Members are entitled to damages, civil penalties, punitive damages, treble damages, nominal damages and/or injunctive relief.

271. **Typicality**. Consistent with Rule 23(a)(3), Plaintiffs' claims are typical of those of other Class and Subclass Members because Plaintiffs' PII and PHI, like that of every other Class and Subclass Member, was compromised in the Data Breach. Moreover, all Plaintiffs and Class and Subclass Members were subjected to Aetna's uniform negligent, unjust, deceptive, unfair, unconscionable, and improper conduct.

272. **Adequacy of Representation**. Consistent with Rule 23(a)(4), Plaintiffs are adequate Class and Subclass representatives because they are members of the Classes and their interests do not conflict with the interests of other Class and Subclass Members that they seek to represent. Plaintiffs are committed to pursuing this matter for the Classes with each Class's collective best interest in mind. Plaintiffs have retained counsel competent and experienced in complex class action litigation of this type and Plaintiffs intend to prosecute this action vigorously. Plaintiffs and their counsel will fairly and adequately protect the Class's and Subclasses' interests.

273. **Predominance**. Consistent with Rule 23(b)(3), Aetna has engaged in a common course of conduct toward Plaintiffs and Class and Subclass Members, in that all the Plaintiffs' and Class and Subclass Members' PII and PHI was unlawfully and inadequately protected in the same

way. The common issues arising from Aetna's conduct affecting Class and Subclass Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

274. **Superiority**. Consistent with Rule 23(b)(3), a class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class and Subclass Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class and Subclass Members would create a risk of inconsistent or varying adjudications with respect to individual Class and Subclass Members, which would establish incompatible standards of conduct for Aetna. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources, the parties' resources, and protects the rights of each Class and Subclass Member. Aetna's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class and Subclass Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

275. The Classes defined above are readily ascertainable from information in Aetna's possession. The Class and Subclasses consist of individuals who received health insurance from Aetna. Thus, identification of the members of the Classes will be reliable and administratively feasible, and adequate notice can be given to Class and Subclass Members directly using information maintained in Aetna's records.

276. Aetna, through its uniform conduct, acted on grounds that apply generally to the Class and each Subclass as a whole, so that class certification, injunctive relief, and corresponding

declaratory relief are appropriate on a class-wide basis. Injunctive relief is necessary to uniformly protect the Classes' data. Plaintiffs seek prospective injunctive relief as a wholly separate remedy from any monetary relief.

277. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Aetna owed a legal duty to Plaintiffs and the Classes to exercise due care in collecting, storing, and safeguarding their PII and PHI;

b. Whether Aetna failed to take commercially reasonable steps to safeguard the PII and PHI of Plaintiffs and the Class Members;

c. Whether Aetna failed to adequately monitor and audit the data security systems of their vendors and business associates, like NationsBenefits;

d. Whether a contract existed between Class and Subclass Members and Aetna, providing that Aetna would implement and maintain reasonable security measures to protect and secure Class and Subclass Members' PII and PHI from unauthorized access and disclosure;

e. Whether Aetna was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiffs and Class and Subclass Members;

f. Whether Plaintiffs and Class Members maintained a confidential relationship with Aetna;

g. Whether Aetna knew or should have known Plaintiffs' and Class Members' PII and PHI was disclosed to Aetna in confidence;

h. Whether Aetna affirmatively disclosed Plaintiffs' and Class Members' PII and PHI to NationsBenefits without consent;

i. Whether Aetna engaged in unfair, unconscionable, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiffs and Class and Subclass Members;

j. Whether Aetna owed a duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class and Subclass Members;

k. Whether Aetna failed to notify Plaintiffs and Class and Subclass Members as soon as practicable and without delay after the Data Breach was discovered;

l. Whether Aetna's delay in informing Plaintiffs and Class and Subclass Members of the Data Breach was unreasonable;

m. Whether Aetna's method of informing Plaintiffs and Class and Subclass Members of the Data Breach was unreasonable;

n. Whether Aetna was unfairly and unjustly enriched as a result of its improper conduct, such that it would be inequitable for Aetna to retain the benefits conferred upon them by Plaintiffs and the other Class Members; and

o. Whether adherence to HIPAA regulations, FTC data security recommendations, industry standards, and measures recommended by data security experts would have reasonably prevented the disclosure of Plaintiffs' and Class and Subclass Members' PII and PHI.

## CLAIMS FOR RELIEF

## COUNT I

### NEGLIGENCE
### (On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, Plaintiffs and the Subclasses)

278. Plaintiffs, individually and on behalf of the Class (or alternatively the Subclasses), repeat and re-allege all preceding allegations as if fully set forth herein.

279. Aetna, as Plaintiffs' and Class Members' health insurer, required Plaintiffs and Class Members to provide Aetna their PII and PHI in order to obtain Aetna's services, specifically health insurance and related benefits. Aetna collected, maintained, and stored Plaintiffs' and Class Members' PII and PHI and used it, as well as shared and transmitted it, to NationsBenefits for commercial gain.

280. Aetna owed a non-delegable duty to Plaintiffs and Class Members to exercise reasonable care to ensure that NationsBenefits, as an Aetna vendor and business associate with whom it shared and transmitted Plaintiffs' and Class Members' PII and PHI, maintained adequate

and commercially reasonable data security practices to ensure the protection of Plaintiffs' and Class Members' PII and PHI.

281. Aetna owed a duty to Plaintiffs and Class Members to exercise reasonable care, which included a responsibility to properly secure and encrypt Plaintiffs' and Class Members' PII and PHI that it exchanged with NationsBenefits and to monitor, audit, and verify the computer, network, and data security measures of NationsBenefits.

282. Aetna owed a duty of care to Plaintiffs and Class Members to provide data security consistent with statutes, regulations, and industry standards, described above, to ensure that it properly secured and encrypted Plaintiffs' and Class Members' PII and PHI that it exchanged with NationsBenefits and that NationsBenefits' systems, networks, and procedures adequately protected Plaintiffs' and Class Members' PII and PHI.

283. Aetna owed Plaintiffs and Class Members a duty to notify them within a reasonable time frame of any breach to their PII and PHI. Aetna also owed a duty to timely and accurately disclose to Plaintiffs and Class Members the scope, nature, and occurrence of the Data Breach. This duty is necessary for Plaintiffs and Class Members to take appropriate measures to protect their PII and PHI, to be vigilant in the face of an increased risk of harm, and to take other necessary steps in an effort to mitigate the fallout of the Data Breach.

284. Aetna's duty to use reasonable care in protecting PII and PHI arose as a result of the common law and the statutes and regulations as well as its own promises regarding privacy and data security to Plaintiffs and Class Members. This duty exists because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices. By collecting and maintaining personal and confidential information of Plaintiffs and Class Members, and acknowledging that this information needed to be kept secure, it was foreseeable that they

would be harmed in the future if Aetna did not protect Plaintiffs' and Class Members' information from threat actors.

285. Aetna's duty of care arose as a result of the special relationship that existed between Aetna and Plaintiffs and Class Members. The special relationship arose because Plaintiffs and Class Members entrusted Aetna with their confidential data as part of the health insurance process. Only Aetna was in a position to ensure that its vendors and business associates had sufficient safeguards to protect against the foreseeable risk that a data breach could occur and would result in substantial harm to Plaintiffs and Class Members.

286. Aetna's duty also arose under HIPAA regulations, which, as described above, applied to Aetna and establish national standards for the protection of patient information, including protected health information, which required Aetna to "reasonably safeguard" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. §164.530(c)(1)-(c)(2). The duty also arose under HIPAA's Privacy rule requirement that Aetna obtain satisfactory assurances from its business associate NationsBenefits that NationsBenefits would appropriately safeguard the protected health information it receives or creates on behalf of Aetna. 45 C.F.R. §§164.502(e), 164.504(e), 164.532(d) and (e). The confidential data at issue in this case constitutes "protected health information" within the meaning of HIPAA.

287. Aetna's duties also arose under Section 5 of the FTC Act, 15 U.S.C. §45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect personal and confidential information. Various FTC publications and data security breach orders further form

the basis of Aetna's duty. In addition, several individual states have enacted statutes based upon the FTC Act that also created a duty.

288. Aetna was subject to an independent duty untethered to any contract between Plaintiffs and Class Members and Aetna.

289. Aetna owed these duties to Plaintiffs and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Aetna knew or should have known would suffer injury-in-fact from its inadequate security protocols. After all, Aetna actively sought and obtained the PII and PHI of Plaintiffs and Class Members.

290. Given the vast amount of highly valuable PII and PHI that Aetna aggregates and makes available to third parties, like NationsBenefits, the risk that unauthorized persons would attempt to gain access to Plaintiffs' and Class Members' PII and PHI and misuse it was foreseeable. Aetna knew or should have known the importance of exercising reasonable care in handling the PII and PHI entrusted to it, including when allowing third parties like NationsBenefits access to Plaintiffs' and Class Members' sensitive PII and PHI.

291. Given the nature of Aetna's business, the sensitivity and value of the PII/PHI it maintains, and the resources at its disposal, Aetna should have identified and foreseen that the third parties they share information with could have vulnerabilities in their systems and prevented the dissemination of Plaintiffs' and Class Members' PII/PHI.

292. It was or should have been reasonably foreseeable to Aetna that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' PII/PHI by failing to ensure that the third parties it shares PII/PHI with design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized

release, disclosure, and dissemination of Plaintiffs' and Class Members' PII/PHI to unauthorized individuals.

293. Indeed, Aetna is no stranger to data breaches at business associates. In 2022, a ransomware attack on a business associate led to the disclosure of PHI of Aetna plan members. In 2020, a phishing attack on a business associate exposed the PHI of Aetna plan members.

294. It was also foreseeable that Aetna's failure to provide timely and adequate notice of the Data Breach would result in injury to Plaintiffs and Class Members.

295. Aetna breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiffs' and Class Members' PII and PHI. And but for Aetna's negligence, Plaintiffs and Class Members would not have been injured. The specific negligent acts and omissions committed by Aetna include, but are not limited to:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs' Class Members' PII and PHI;

b. Failing to properly secure and encrypt Plaintiffs' and Class Members' PII and PHI that it exchanged with NationsBenefits;

c. Failing to ensure that NationsBenefits, as an Aetna vendor and business associate with whom it shared and transmitted Plaintiffs' and Class Members' PII and PHI, maintained adequate and commercially reasonable data security practices to ensure the protection of Plaintiffs' and Class Members' PII and PHI

d. Failing to comply with – and thus violating – HIPAA and its regulations;

e. Failing to comply with – and thus violating – HITECH and its regulations;

f. Failing to comply with – and thus violating – FTC Act and its regulations;

g. Failing to adequately monitor the security of its networks and systems;

h. Failing to have in place mitigation policies and procedures;

i. Allowing unauthorized access to Plaintiffs' and Class Members' PII and PHI;

j. Failing to detect in a timely manner that Plaintiffs' and Class Members' PII and PHI had been compromised; and

k. Failing to timely notify Plaintiffs' Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

296. It was foreseeable that Aetna's failure to use reasonable measures to protect Plaintiffs' and Class Members' PII and PHI would result in injury to Plaintiffs and Class Members. Furthermore, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry. It was therefore foreseeable that the failure to adequately safeguard Plaintiffs' and Class Members' PII and PHI would result in one or more types of injuries to Plaintiffs and Class Members.

297. Plaintiffs and Class Members had and have no ability to protect their PII/PHI that was, or remains, in Aetna's possession and control.

298. But for Aetna's negligent conduct or breach of the above-described duties, Plaintiffs' and Class Members' PII/PHI would not have been compromised. The PII/PHI of Plaintiffs and the Class was accessed and stolen as the proximate result of Aetna's failure to exercise reasonable care in safeguarding, securing, and protecting such PII/PHI by, *inter alia*, monitoring, auditing, and ensuring that third parties it contracts with and shares PII/PHI with adopt, implement, and maintain appropriate security measures.

299. Aetna's failure to take proper security measures and to monitor, audit, and ensure that its third-party vendors and business associates took proper security measures to protect sensitive PII and PHI of Plaintiffs and Class Members created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Plaintiffs' and Class Members' PII and PHI.

300. Neither Plaintiffs nor the other Class Members contributed to the Data Breach and subsequent misuse of their PII and PHI.

301. As a direct and proximate result of Aetna's negligence, Plaintiffs and the Class have suffered and will continue to suffer injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their PII and PHI, and monetary and non-monetary damages. Specifically, Plaintiffs and Class Members have suffered and will continue to suffer a range of injuries, including but not limited to: (1) actual identity theft; (2) a substantially increased and imminent risk of identity theft; (3) the loss of the opportunity to determine how their PII and PHI is used; (4) the compromise, publication, and/or theft of their PII and PHI; (5) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and PHI; (6) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft; (7) the continued risk to their PII and PHI, which remain in Aetna's possession and is subject to further unauthorized disclosures so long as Aetna fails to undertake appropriate and adequate measures to protect the PII and PHI in its possession; (8) overpayment for the goods and services that were received without adequate data security; (9) lost value of their PII and PHI; (10) emotional distress directly and proximately caused by Aetna's wrongful conduct; and (11) future expenditures of time, effort, and money that will be spent trying to prevent, detect, contest, and repair the impact of the Data Breach.

302. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including, but not limited to, compensatory and consequential damages and equitable relief.

## COUNT II

**NEGLIGENCE PER SE**
**(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, Plaintiffs and the Subclasses)**

303. Plaintiffs, individually and on behalf of the Class (or alternatively the Subclasses), repeat and re-allege all preceding allegations in paragraphs 1-263 as if fully set forth herein.

304. Aetna is an entity covered by HIPAA (45 C.F.R. §160.102) and as such is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

305. Under HIPAA, Aetna has a duty to use reasonable security measures to "reasonably safeguard" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. §164.530(c)(1)-(c)(2). HIPAA also requires Aetna to obtain satisfactory assurances that its business associates would appropriately safeguard the protected health information it receives or creates on behalf of Aetna. 45 CFR §164.502(e), 164.504(e), 164.532(d) and (e). Some or all of the information at issue in this case constitutes "protected health information" within the meaning of HIPAA. 45 C.F.R. §164.530(c)(1). NationsBenefits constitutes a "business associate" within the meaning of HIPAA.

306. HIPAA further requires Aetna to disclose the unauthorized access and theft of the PII and PHI to Plaintiffs and Class Members "without unreasonable delay" so that Plaintiffs and Class Members can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PII and PHI. *See* 45 C.F.R. §§164.404, 406, 410. *See also* 42 U.S.C. §17932.

307. Aetna violated HIPAA by failing to reasonably protect Plaintiffs' and Class Members' PII and PHI, as described herein.

308. Plaintiffs and Class Members are within the class of persons that the HIPAA was intended to protect. The harm Plaintiffs and Class Members have suffered and will suffer as a result of Aetna's breach of its duties is precisely the type of harm HIPAA is intended to guard against.

309. Under the FTC Act, Aetna has a duty to employ reasonable security measures. Specifically, this statute prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data. 15 U.S.C. §45(a)(1).

310. The FTC publications and orders described above also form part of the basis of Aetna's duty in this regard.

311. Aetna violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and PHI and not complying with applicable industry standards. Aetna's conduct was particularly unreasonable given the nature and amount of PII and PHI it obtained, stored, and disseminated, and the foreseeable consequences of a data breach involving protected health information and companies as large as Aetna, including, specifically, the immense damages that would result to Plaintiffs and Class Members.

312. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect. Moreover, the harm Plaintiffs and Class Members have suffered and will suffer as a result of Aetna's breach of its duties is precisely the type of harm the FTC Act is intended to guard against. The FTC has pursued numerous enforcement actions against businesses that – because of their failure to employ reasonable data security measures and avoid unfair and

deceptive practices – caused the very same injuries that Aetna inflicted upon Plaintiffs and Class Members.

313. Aetna also violated the following consumer protection, privacy, and data breach notification statutes: Conn. Gen. Stat. Ann. §§42-110a, *et seq.*; Conn. Gen. Stat. Ann. §§38a-815, 816(1)-(2); Conn. Gen. Stat. Ann. §38a-988; Fla. Stat. §§501.201, *et seq.*; Fla. Stat. §501.171; Ga. Code Ann. §§10-1-370, *et seq.*; Ga. Code Ann. §33-39-14; Ga. Code Ann. §§10-1-910, *et seq.*; 815 Ill. Comp. Stat. §§505/1, *et seq.*; 815 Ill. Comp. Stat. Ann. §510/2; 215 Ill. Comp. Stat. 5/1014; 815 Ill. Comp. Stat. §530/1, *et seq.*; 815 Ill. Comp. Stat. §505/2RR; Mass. Gen. Laws 93H §1, *et seq.*; Mich. Comp. Laws Ann. §§445.903, *et seq.*; Mich. Comp. Laws Ann. §§445.72; Nev. Rev. Stat. §§598.0901, *et seq.*; Nev. Rev. Stat. §603A.010, *et seq.*; N.Y. Gen. Bus. Law §349; N.Y. Gen. Bus. Law §899-aa; N.D. Cent. Code §§51-15-01, *et seq.*; N.D. Cent. Code §§26.1-04-01, *et seq.*; N.D. Cent. Code §51-30-01, *et seq.*; Ohio Rev. Code §§1345.01, *et seq.*; Ohio Rev. Code §1349.19; 15 Okla. Stat. §§751, *et seq.*; and 24 Okla. Stat. §161, *et seq.* Plaintiffs and Class Members are within the class of persons that these statutes are intended to protect. Moreover, the harm Plaintiffs and Class Members have suffered and will suffer as a result of Aetna's breach of its duties is precisely the type of harm that these statutes are intended to guard against.

314. As a direct and proximate result of Aetna's negligence per se, Plaintiffs and the Class have suffered and will continue to suffer injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their PII and PHI, and monetary and non-monetary damages, as described herein. Specifically, Plaintiffs and Class Members have suffered and will continue to suffer a range of injuries, including, but not limited to: (1) actual identity theft; (2) a substantially increased and imminent risk of identity theft; (3) the loss of the opportunity to determine how their PII and PHI is used; (4) the compromise, publication, and/or

theft of their PII and PHI; (5) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and PHI; (6) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft; (7) the continued risk to their PII and PHI, which remain in Aetna's possession and is subject to further unauthorized disclosures so long as Aetna fails to undertake appropriate and adequate measures to protect the PII and PHI in its possession; (8) overpayment for the goods and services that were received without adequate data security; (9) lost value of their PII and PHI; (10) emotional distress directly and proximately caused by Aetna's wrongful conduct; and (11) future expenditures of time, effort, and money that will be spent trying to prevent, detect, contest, and repair the impact of the Data Breach.

315. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including, but not limited to, compensatory and consequential damages and equitable relief.

## COUNT III

### BREACH OF CONTRACT
### (On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, Plaintiffs and the Subclasses)

316. Plaintiffs, individually and on behalf of the Class (or alternatively the Subclasses), repeat and re-allege all preceding allegations in paragraphs 1-263 as if fully set forth herein.

317. Aetna and Plaintiffs and Class Members entered into contracts wherein Aetna agreed to provide health insurance to its customers.

318. Upon information and belief, Aetna either directly or by incorporating the Privacy Policy by reference promised to safeguard, secure, and protect Plaintiffs' and Class Members' PII

and PHI, promised to comply with all federal and state laws and regulations, including HIPAA, and promised to timely and accurately provide notification if Plaintiffs' and Class Members' PII/PHI had been breached, compromised, or stolen.

319. Plaintiffs and Class Members fully performed their obligations under the contracts.

320. Aetna breached its contracts when it failed to safeguard, secure, and protect the PII/PHI of Plaintiffs and Class Members by failing to secure and encrypt Plaintiffs' and Class Members' PII and PHI Aetna shared and transmitted to NationsBenefits and to verify, monitor, and audit NationsBenefits to ensure it had adequate measures to safeguard, secure, and protect Plaintiffs' and Class Members' PII and PHI.

321. Aetna breached the contracts it made with Plaintiffs and Class Members by failing to safeguard and protect their PII/PHI and by failing to provide timely and accurate notice to them that their PII/PHI was compromised as a result of the Data Breach.

322. Aetna further breached the contracts with Plaintiffs and Class Members by failing to comply with its promise to abide by HIPAA.

323. Aetna further breached the contracts with Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information Aetna created, received, maintained, and transmitted in violation of 45 CFR 164.306(a)(1).

324. Aetna further breached the contracts with Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1).

325. Aetna further breached the contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2).

326. Aetna's failures to meet these promises constitute breaches of the contracts.

327. Furthermore, the failure to meet its confidentiality and privacy obligations resulted in Aetna providing services to Plaintiffs and Class Members that were of a diminished value.

328. As a direct and proximate result of Aetna's breach of its contract, Plaintiffs and Class Members are at a substantial, impending, and imminent risk of identity theft, and they have been forced to take mitigation steps, to ensure their personal and financial safety.

329. As a direct and proximate result of Aetna's above-described breach of contract, Plaintiffs and the Class have suffered and will continue to suffer injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their PII and PHI, and monetary and non-monetary damages. Specifically, Plaintiffs and Class Members have suffered and will continue to suffer a range of injuries, including but not limited to: (1) actual identity theft; (2) a substantially increased and imminent risk of identity theft; (3) the loss of the opportunity to determine how their PII and PHI is used; (4) the compromise, publication, and/or theft of their PII and PHI; (5) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and PHI; (6) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft; (7) the continued risk to their PII and PHI, which remain in Aetna's possession and is subject to further unauthorized disclosures so long as Aetna fails to undertake appropriate and adequate measures to protect the PII and PHI in its possession; (8) overpayment for the goods and services that were received without adequate data security; and (9) future expenditures of time, effort, and money that will be spent trying to prevent, detect, contest, and repair the impact of the Data Breach.

330. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including, but not limited to, actual, consequential, and nominal damages and equitable relief.

## COUNT IV

### UNJUST ENRICHMENT
### (On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, Plaintiffs and the Subclasses)

331. Plaintiffs, individually and on behalf of the Class (or alternatively the Subclasses), repeat and re-allege all preceding allegations in paragraphs 1-263 as if fully set forth herein.

332. This cause of action is plead in the alternative to the breach of contract theory.

333. For years and continuing to today, Aetna's business model has depended upon its health plan holders entrusting it with their PII and PHI. Trust and confidence are critical and central to the services provided by Aetna. Unbeknownst to Plaintiffs and Class Members, however, Aetna failed to secure and encrypt Plaintiffs' and Class Members' PII and PHI that it transmitted to NationsBenefits and failed to ensure its vendors and business associates reasonably or adequately secured, safeguarded, and otherwise protected Plaintiffs' and Class Members' PII and PHI. Aetna's deficiencies described herein were contrary to their security messaging.

334. Plaintiffs and Class Members engaged Aetna for health insurance and other benefits and provided Aetna with, and allowed Aetna to collect, their PII and PHI on the mistaken belief that Aetna complied with its duty to safeguard and protect health plan holders' PII and PHI. Putting its short-term profit ahead of safeguarding PII and PHI, and unbeknownst to Plaintiffs and Class Members, Aetna knowingly sacrificed security in favor of collecting moneys Aetna believed it was owed. Aetna knew that the manner in which it maintained and transmitted Plaintiffs' and Class Members' PII and PHI violated its fundamental duties to Plaintiffs and Class Members by

disregarding its statutory and regulatory duties and industry-standard security protocols to ensure confidential information was securely transmitted and stored.

335. Aetna had within its exclusive knowledge at all relevant times the fact that its vendors and business associates failed to implement adequate security measures to keep health plan holders' PII and PHI secure. This information was not available to Plaintiffs, Class Members, or the public at large.

336. Aetna also knew that Plaintiffs and Class Members expected that their information would be kept secure against known security risks and that the security protocols of any vendors or business associates used by Aetna would be thoroughly vetted before they received health plan holders' PII and PHI. And based on this expectation and trust, Aetna knew that Plaintiffs and Class Members would not have disclosed health information to it and would have chosen a different provider for services.

337. Plaintiffs and Class Members did not expect that Aetna would store or transmit their PII and PHI insecurely or engage another benefits provider, NationsBenefits, that employed substantially deficient security protocols and would store sensitive PII and PHI.

338. Plaintiffs and Class Members conferred a monetary benefit on Aetna, by paying money for healthcare benefits and other services, a portion of which was intended to have been used by Aetna for data security measures to ensure the security of Plaintiffs' and Class Members' PII and PHI, including by monitoring and auditing NationsBenefits networks and data security measures. Plaintiffs and Class Members further conferred a benefit on Aetna by entrusting their PII and PHI to Aetna from which Aetna derived profits.

339. Aetna enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII and PHI. Instead of providing

a reasonable level of security that would have protected Plaintiffs' and Class Members' PII and PHI, Aetna instead calculated to avoid its data security obligations at the expense of Plaintiffs and Class Members by avoiding its network and data security monitoring and auditing measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Aetna's failure to ensure adequate security.

340. Under the principles of equity and good conscience, Aetna should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Aetna failed to implement appropriate data security measures that are mandated by law, regulation, and industry standards, including monitoring and auditing NationsBenefits' network and data security measures.

341. Aetna acquired the monetary benefit through inequitable means in that Aetna failed to disclose the inadequate security practices, previously alleged, and failed to ensure NationsBenefits maintained adequate data security measures.

342. Had Plaintiffs and Class Members known about Aetna's practice of sharing their PII and PHI with vendors and business associates who were unequipped to protect that data and insecurely transmitting PII and PHI that had no bearing on providing services, Plaintiffs and Class Members would not have engaged Aetna to provide health insurance benefits and other services and would never have provided Aetna with their PII and PHI.

343. By withholding these material facts, Aetna put its own interests ahead of its health plan holders' interests and benefited itself to the detriment of Plaintiffs and Class Members.

344. As a result of its conduct as alleged herein, Aetna sold more health insurance and other services than it otherwise would have and was able to charge Plaintiffs and Class Members when it otherwise could not have. Aetna was unjustly enriched by charging and collecting for those benefits and other services to the detriment of Plaintiffs and Class Members.

345. Aetna's defective security and its unfair and deceptive conduct have, among other things, caused Plaintiffs and Class Members to unfairly incur substantial time and/or costs to mitigate and monitor the use of their private PII and PHI.

346. Plaintiffs and Class Members have no adequate remedy at law.

347. As a direct and proximate result of Aetna's conduct, Plaintiffs and the Class have suffered and will continue to suffer injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their PII and PHI, and monetary and non-monetary damages. Specifically, Plaintiffs and Class Members have suffered and will continue to suffer a range of injuries, including but not limited to: (1) actual identity theft; (2) a substantially increased and imminent risk of identity theft; (3) the loss of the opportunity to determine how their PII and PHI is used; (4) the compromise, publication, and/or theft of their PII and PHI; (5) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and PHI; (6) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (7) the continued risk to their PII and PHI, which remain in Aetna's possession and is subject to further unauthorized disclosures so long as Aetna fails to undertake appropriate and adequate measures to protect the PII and PHI in its possession; (8) overpayment for the good and services that were received without adequate data security; and (9) future expenditures of time, effort, and money that will be spent trying to prevent, detect, contest, and repair the impact of the Data Breach.

348. Plaintiffs and the Class seek all monetary and non-monetary relief allowed by law, including equitable relief such that Aetna should be compelled to disgorge into a common fund or

constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that it unjustly received from Plaintiffs and Class Members.

## COUNT V

### BREACH OF CONFIDENCE
### (On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, Plaintiffs and the Subclasses)

349. Plaintiffs, individually and on behalf of the Class (or alternatively the Subclass), repeat and re-allege all preceding allegations in paragraphs 1-263 as if fully set forth herein.

350. Plaintiffs and Class Members maintained a confidential relationship with Aetna whereby Aetna undertook a duty not to disclose to unauthorized third parties the PII and PHI provided by Plaintiffs and Class Members to Aetna. Such PII and PHI was confidential and immutable, highly personal and sensitive, and not generally known.

351. Aetna knew Plaintiffs' and Class Members' PII and PHI was being disclosed in confidence and understood the confidence was to be maintained, including by expressly and implicitly agreed to protect the confidentiality and security of the PII and PHI it collected, stored, and maintained.

352. Aetna affirmatively disclosed Plaintiffs' and Class Members' PII and PHI to NationsBenefits without their consent.

353. As a result of the Data Breach, there was an unauthorized disclosure of Plaintiffs' and Class Members' PII and PHI. The unauthorized disclosure occurred because Aetna: (a) disclosed Plaintiffs' and Class Members' PII and PHI to NationsBenefits without a legitimate business reason to do so and without consent; and (b) failed to implement and maintain reasonable safeguards to protect the PII and PHI, including by securing and encrypting the PII and PHI that Aetna transmitted to NationsBenefits and verifying, monitoring, and auditing that NationsBenefits

maintained reasonably adequate data security measures to protect Plaintiffs' and Class Members' PII and PHI.

354. NationsBenefits did not need access to Plaintiffs' and Class Members' PII and PHI at all unless and until they actually decided to obtain NationsBenefits' services. But Aetna nevertheless regularly and affirmatively provided full account information that included PII and PHI, apparently because it was more expedient than waiting until a member actually wanted to obtain NationsBenefits' services.

355. Plaintiffs and Class Members were harmed by way of an unconsented disclosure of their confidential information to an unauthorized third party.

356. As a direct and proximate result of Aetna's breach of confidence, Plaintiffs and Class Members suffered injury and sustained actual losses and damages as alleged herein.

357. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including compensatory or nominal damages and equitable relief.

## COUNT VI

### CONNECTICUT UNFAIR TRADE PRACTICES ACT
### Conn. Gen. Stat. Ann. §§42-110a, *et seq*.
### (On Behalf of Plaintiff Titcomb and the Connecticut Subclass)

358. Plaintiff Titcomb ("Plaintiff" for purposes of this Count), individually and on behalf of the Connecticut Subclass, repeats and re-alleges all preceding allegations in paragraphs 1-263 as if fully set forth herein.

359. The Connecticut Unfair Trade Practices Act ("CUTPA") provides that "[n]o person shall engage in unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce." Conn. Gen. Stat. Ann. §42-110b(a). CUTPA expressly provides that consideration be given to interpretations by the FTC relating to Section 5 of the FTC Act. *See* Conn. Gen. Stat. Ann. §42-110b(b).

360. Aetna is a "person" as defined by Conn. Gen. Stat. Ann. §42-110a(3).

361. Plaintiff and Connecticut Subclass Members are actual consumers of Aetna's goods or services and qualify as a "person who suffers any ascertainable loss of money or property, real or personal, as a result of the use or employment of a method, act or practice prohibited by section 42-110b" under Conn. Gen. Stat. Ann. §42-110g.

362. Aetna advertised, offered, or sold goods or services in Connecticut and therefore engaged in trade or commerce directly or indirectly affecting the people of Connecticut. Conn. Gen. Stat. §42-110a(4).

363. Aetna engaged in deceptive, unfair, and unlawful acts and practices in the conduct of trade or commerce, in violation of CUTPA.

364. Aetna's deceptive acts and practices include:

a. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Connecticut Subclass Members' PII and PHI;

b. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Connecticut Subclass Members' PII and PHI, including duties imposed by the FTC Act, HIPAA, the Connecticut Insurance Information and Privacy Protection Act (Conn. Gen. Stat. Ann. §38a-988), and the Connecticut data breach notification statute (Conn. Gen. Stat. Ann. §42-471);

c. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Connecticut Subclass Members' PII and PHI, including by failing to reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and Connecticut Subclass Members' PII and PHI; and

d. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Connecticut Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as the Connecticut Insurance Information and Privacy Protection Act (Conn. Gen. Stat. Ann. §38a-988).

365. Aetna's unfair acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Connecticut Subclass Members' PII and PHI, including by failing to properly secure and encrypt Plaintiff's and Connecticut Subclass Members' PII and PHI exchanged with NationsBenefits and failing to reasonably ensure its vendors and business associates reasonably and adequately secured Plaintiff's and Connecticut Subclass Members' PII and PHI;

b. Disclosing Plaintiff's and Connecticut Subclass Members' PII and PHI to NationsBenefits without a legitimate business reason to do so;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Connecticut Subclass Members' PII and PHI, including duties imposed by the FTC Act, HIPAA, and the Connecticut Insurance Information and Privacy Protection Act (Conn. Gen. Stat. Ann. §38a-988); and

d. Failing to comply with the duties imposed by Conn. Gen. Stat. Ann. §36a-701b and disclose the Data Breach to Plaintiff and the Connecticut Subclass in a timely and accurate manner.

366. Aetna's conduct constitutes unfair methods of competition and unfair practices within the meaning of CUTPA because it is immoral, unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers and businesses, and provided no benefit to consumers or competition. Aetna cut corners and minimized costs by failing to reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and Connecticut Subclass Members' PII and PHI. Further, the injuries suffered by Plaintiff and the Connecticut Subclass Members are not outweighed by any countervailing benefits to consumers or competition. And, because Aetna is solely responsible for reasonably ensuring its vendors and business associates reasonably or adequately secured Plaintiff's and Connecticut Subclass Members' PII and PHI, there is no way Plaintiff and the Connecticut Subclass Members could have known about Aetna's inadequate data security practices. By withholding important information from consumers about the inadequacy of its data security measures, Aetna created an asymmetry of information

between it and consumers that precluded consumers from taking action to avoid or mitigate injury. There were reasonably available alternatives to further Aetna's legitimate business interests.

367. Aetna's conduct constitutes unfair practices within the meaning of CUTPA because it undermines public policy that businesses protect PII and PHI, as reflected in the FTC Act and HIPAA, as well as the Connecticut Insurance Information and Privacy Protection Act (Conn. Gen. Stat. Ann. §38a-988).

368. Aetna's acts and practices are unfair because Aetna's failure to disclose the inadequacies in its data security measures materially interfered with consumers' decision-making in their transactions with Aetna. Further, Aetna took unreasonable advantage of consumers' lack of understanding about the material risks and costs in their transactions with Aetna and consumers' inability to protect themselves due to the asymmetry of information concerning Aetna's data security practices.

369. The above deceptive or unfair acts and practices by Aetna also violated Connecticut's Unfair Insurance Practices Act, Conn. Gen. Stat. Ann. §§38a-815, 816(1)-(2).

370. Aetna's misrepresentations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Aetna's data security measures and ability to protect the confidentiality of consumers' PII and PHI.

371. Aetna's acts and practices, including its material omissions, were likely to, and did in fact, deceive and mislead members of the public, including consumers acting reasonably under the circumstances, to their detriment.

372. Aetna intended to mislead Plaintiff and Connecticut Subclass Members and induce them to rely on its misrepresentations and omissions.

373. Aetna had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extent of the PII and PHI in their possession. This duty arose because members of the public, including Plaintiff and the Connecticut Subclass Members, bestowed trust and confidence in Aetna to keep their PII and PHI secure. Aetna's duty to disclose also arose from its possession of exclusive knowledge regarding the security of its vendors' and business associates' systems.

374. Had Aetna disclosed to Plaintiff and the Connecticut Subclass Members that it did not adequately verify, monitor, and audit the data security measures of its vendors and business associates, Aetna would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Aetna was trusted with sensitive and valuable PII and PHI regarding millions of consumers, including Plaintiff and the Connecticut Subclass Members. Aetna accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Connecticut Subclass Members acted reasonably in relying on Aetna's misrepresentations and omissions, the truth of which they could not have discovered.

375. Aetna acted intentionally, knowingly, and maliciously to violate CUTPA and recklessly disregarded Plaintiff's and Connecticut Subclass Members' rights.

376. Aetna's deceptive and unfair trade practices significantly impact the public, because many members of the public are actual or potential consumers of Aetna's services and the Data Breach affected millions of Americans, which include members of the Connecticut Subclass.

377. Aetna's violations present a continuing risk to Plaintiff and the Connecticut Subclass as well as to the general public.

378. As a direct and proximate result of Aetna's deceptive or unfair trade practices, Plaintiff and the Connecticut Subclass Members have suffered and will continue to suffer injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their PII and PHI, and monetary and non-monetary damages. Specifically, Plaintiff and Connecticut Subclass Members have suffered and will continue to suffer a range of injuries, including but not limited to: (1) actual identity theft; (2) a substantially increased and imminent risk of identity theft; (3) the loss of the opportunity to determine how their PII and PHI is used; (4) the compromise, publication, and/or theft of their PII and PHI; (5) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and PHI; (6) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft; (7) the continued risk to their PII and PHI, which remain in Aetna's possession and is subject to further unauthorized disclosures so long as Aetna fails to undertake appropriate and adequate measures to protect the PII and PHI in its possession; (8) overpayment for the goods and services that were received without adequate data security; (9) lost value of their PII and PHI; and (10) future expenditures of time, effort, and money that will be spent trying to prevent, detect, contest, and repair the impact of the Data Breach, and thereby suffered ascertainable economic loss.

379. Plaintiff and the Connecticut Subclass seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, equitable relief, and attorneys' fees and costs.

## COUNT VII

### FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT
### Fla. Stat. §§501.201, *et seq*.
### (On Behalf of Plaintiffs Luciano and Veazey and the Florida Subclass)

380. Plaintiffs Luciano and Veazey ("Plaintiffs" for purposes of this Count), individually and on behalf of the Florida Subclass Members, repeat and re-allege all preceding allegations in paragraphs 1-263 as if fully set forth herein.

381. The Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"), Fla. Stat. §§501.201, *et seq*., prohibits unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of trade or commerce. *See* Fla. Stat. §501.204(1). FDUTPA expressly provides that consideration be given to interpretations by the FTC relating to Section 5 of the FTC Act. *See* Fla. Stat. §501.204(2); *see also* Fla. Stat. §§501.202(3), 501.203(3)(a)-(c).

382. Plaintiffs and the Florida Subclass Members are "consumers" as defined by Fla. Stat. §501.203(7) and Plaintiffs and each Florida Subclass Member are aggrieved and have suffered a loss under Fla. Stat. §501.211(1)-(2) as a result of Aetna's violations of FDUTPA.

383. Aetna is engaged in a trade or commerce within the meaning of Fla. Stat. §501.203(8).

384. Aetna advertised, offered, or sold goods or services in Florida and engaged in trade or commerce directly or indirectly affecting the citizens of Florida.

385. Plaintiffs and Florida Subclass Members are Aetna health plan holders located in Florida, where Aetna is authorized to do business. The conduct constituting Aetna's deceptive, unfair, and unconscionable acts and practices under this claim occurred primarily and substantially in Florida because Aetna is authorized to do business in Florida, and Aetna's unlawful conduct:

(a) foreseeably impacted consumers residing in Florida whose PII and PHI was compromised in the Data Breach; and (b) otherwise interfered with trade or commerce in Florida.

386. Aetna engaged in unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of trade and commerce in violation of Fla. Stat. §501.204(1).

387. Aetna's deceptive acts and practices include:

a. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Florida Subclass Members' PII and PHI;

b. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Florida Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as the Florida Information Protection Act (Fla. Stat. §501.171);

c. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Florida Subclass Members' PII and PHI, including by failing to reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiffs' and Florida Subclass Members' PII and PHI; and

d. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Florida Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as the Florida Information Protection Act (Fla. Stat. §501.171).

388. Aetna's unfair or unconscionable acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Florida Subclass Members' PII and PHI, including by failing to properly secure and encrypt Plaintiffs' and Florida Subclass Members' PII and PHI exchanged with NationsBenefits and failing to reasonably ensure its vendors and business associates reasonably and adequately secured Plaintiffs' and Florida Subclass Members' PII and PHI;

b. Disclosing Plaintiffs' and Florida Subclass Members' PII and PHI to NationsBenefits without a legitimate business reason to do so;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Florida Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA; and

d. Failing to comply with the duties imposed by the Florida Information Protection Act (Fla. Stat. §501.171) and disclose the Data Breach to Plaintiffs and the Florida Subclass Members in a timely and accurate manner.

389. Aetna's conduct constitutes unfair methods of competition or unfair or unconscionable practices within the meaning of FDUTPA because it is immoral, unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers and businesses, and provided no benefit to consumers or competition. Aetna cut corners and minimized costs by failing to reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiffs' and Florida Subclass Members' PII and PHI. Further, the injuries suffered by Plaintiffs and the Florida Subclass Members are not outweighed by any countervailing benefits to consumers or competition. And, because Aetna is solely responsible for reasonably ensuring its vendors and business associates reasonably or adequately secured Plaintiffs' and Florida Subclass Members' PII and PHI, there is no way Plaintiffs and the Florida Subclass Members could have known about Aetna's inadequate data security practices. By withholding important information from consumers about the inadequacy of its data security, Aetna created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury. There were reasonably available alternatives to further Aetna's legitimate business interests.

390. Aetna's conduct constitutes unfair practices within the meaning of FDUTPA because it undermines public policy that businesses protect PII and PHI, as reflected in the FTC Act and HIPAA as well as the Florida Information Protection Act (Fla. Stat. §501.171).

391. Aetna's acts and practices are unfair or unconscionable because Aetna's failure to disclose the inadequacies in its data security measures materially interfered with consumers'

decision-making in their transactions with Aetna. Further, Aetna took unreasonable advantage of consumers' lack of understanding about the material risks and costs in their transactions with Aetna and consumers' inability to protect themselves due to the asymmetry of information concerning Aetna's data security practices.

392. Aetna's misrepresentations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Aetna's data security measures and ability to protect the confidentiality of consumers' PII and PHI.

393. Aetna's acts and practices, including its material omissions, were likely to, and did in fact, deceive and mislead members of the public, including consumers acting reasonably under the circumstances, to their detriment.

394. Aetna intended to mislead Plaintiffs and Florida Subclass Members and induce them to rely on its misrepresentations and omissions.

395. Aetna had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extent of the PII and PHI in their possession. This duty arose because members of the public, including Plaintiff and the Florida Subclass, bestowed trust and confidence in Aetna to keep their PII and PHI secure. Aetna's duty to disclose also arose from its possession of exclusive knowledge regarding the security of its vendors' and business associates' systems.

396. Had Aetna disclosed to Plaintiff and the Florida Subclass Members that it did not adequately verify, monitor, and audit the data security measures of its vendors and business associates, Aetna would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Aetna was trusted with sensitive and valuable PII and PHI regarding millions of consumers, including Plaintiffs and the

Florida Subclass. Aetna accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiffs and the Florida Subclass Members acted reasonably in relying on Aetna's misrepresentations and omissions, the truth of which they could not have discovered.

397. Aetna acted intentionally, knowingly, and maliciously to violate FDUTPA, and recklessly disregarded Plaintiffs' and Florida Subclass Members' rights.

398. Aetna's violations present a continuing risk to Plaintiffs and the Florida Subclass Members as well as to the general public.

399. As a direct and proximate result of Aetna's deceptive, unfair, or unconscionable acts and practices, Plaintiffs and the Florida Subclass Members have suffered and will continue to suffer injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their PII and PHI, and monetary and non-monetary damages. Specifically, Plaintiffs and Florida Subclass Members have suffered and will continue to suffer a range of injuries, including but not limited to: (1) actual identity theft; (2) a substantially increased and imminent risk of identity theft; (3) the loss of the opportunity to determine how their PII and PHI is used; (4) the compromise, publication, and/or theft of their PII and PHI; (5) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and PHI; (6) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft; (7) the continued risk to their PII and PHI, which remain in Aetna's possession and is subject to further unauthorized disclosures so long as Aetna fails to undertake appropriate and adequate measures to protect the PII and PHI in its

possession; (8) overpayment for the goods and services that were received without adequate data security; (9) lost value of their PII and PHI; and (10) future expenditures of time, effort, and money that will be spent trying to prevent, detect, contest, and repair the impact of the Data Breach, and thereby suffered ascertainable economic loss.

400. Plaintiff and the Florida Subclass seek all monetary and non-monetary relief allowed by law, including damages, equitable relief, and attorneys' fees and costs.

## COUNT VIII

### GEORGIA UNIFORM DECEPTIVE PRACTICES ACT
### Ga. Code Ann. §§10-1-370, *et seq*.
### (On Behalf of Plaintiff Peffley-Wilson and the Georgia Subclass)

401. Plaintiff Peffley-Wilson ("Plaintiff" for purposes of this Count), individually and on behalf of the Georgia Subclass, repeats and re-alleges all preceding allegations in paragraphs 1-263 as if fully set forth herein.

402. Aetna, Plaintiff, and each member of the Georgia Subclass are "persons" within the meaning of Ga. Code Ann. §10-1-371(5) of the Georgia Uniform Deceptive Trade Practices Act ("Georgia UDTPA").

403. Aetna engaged in deceptive trade practices in the conduct of its business, in violation of Ga. Code Ann. §10-1-372(a), including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

404. Aetna's deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Georgia Subclass Members' PII and PHI, including by failing to properly secure and encrypt Plaintiff's and Georgia Subclass Members' PII and PHI exchanged with NationsBenefits and failing to reasonably ensure its vendors and business associates reasonably and adequately secured Plaintiff's and Georgia Subclass Members' PII and PHI;

b. Disclosing Plaintiff's and Georgia Subclass Members' PII and PHI to NationsBenefits without a legitimate business reason to do so;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and the Georgia Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as the Georgia Insurance Information and Privacy Protection Act (Ga. Code Ann. §33-39-14) and the Georgia Personal Identity Protection Act (Ga. Code Ann. §§10-1-910, *et seq*.);

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and the Georgia Subclass Members' PII and PHI;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and the Georgia Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as the Georgia Insurance Information and Privacy Protection Act (Ga. Code Ann. §33-39-14) and the Georgia Personal Identity Protection Act (Ga. Code Ann. §§10-1-910, *et seq*.);

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and the Georgia Subclass Members' PII and PHI, including by failing to reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and Georgia Subclass Members' PII and PHI; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and the Georgia Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as the Georgia Insurance Information and Privacy Protection Act (Ga. Code Ann. §33-39-14) and the Georgia Personal Identity Protection Act (Ga. Code Ann. §§10-1-910, *et seq*.).

405. Aetna's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Aetna's data security and ability to protect the confidentiality of consumers' PII and PHI.

406. Aetna intended to mislead Plaintiff and the Georgia Subclass Members and induce them to rely on its misrepresentations and omissions.

407. In the course of its business, Aetna engaged in activities with a tendency or capacity to deceive.

408. Aetna acted intentionally, knowingly, and maliciously to violate Georgia's UDTPA, and recklessly disregarded Plaintiff's and the Georgia Subclass Members' rights.

409. Aetna had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extent of the PII and PHI in its possession. This duty arose because members of the public, including Plaintiff and the Georgia Subclass Members, bestowed trust and confidence in Aetna to keep their PII and PHI secure. Aetna's duty to disclose also arose from its possession of exclusive knowledge regarding the security of its vendors' and business associates' systems.

410. Had Aetna disclosed to Plaintiff and the Georgia Subclass Members that it did not adequately verify, monitor, and audit the data security measures of its vendors and business associates, Aetna would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Aetna was trusted with sensitive and valuable PII and PHI regarding millions of consumers, including Plaintiff and the Georgia Subclass Members. Aetna accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the

Georgia Subclass Members acted reasonably in relying on Aetna's misrepresentations and omissions, the truth of which they could not have discovered.

411. Aetna's violations present a continuing risk to Plaintiff and the Georgia Subclass Members as well as to the general public.

412. As a direct and proximate result of Aetna's deceptive trade practices, Plaintiff and the Georgia Subclass Members have suffered and will continue to suffer injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their PII and PHI, and monetary and non-monetary damages. Specifically, Plaintiff and Georgia Subclass Members have suffered and will continue to suffer a range of injuries, including, but not limited to: (1) actual identity theft; (2) a substantially increased and imminent risk of identity theft; (3) the loss of the opportunity to determine how their PII and PHI is used; (4) the compromise, publication, and/or theft of their PII and PHI; (5) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and PHI; (6) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft; (7) the continued risk to their PII and PHI, which remain in Aetna's possession and is subject to further unauthorized disclosures so long as Aetna fails to undertake appropriate and adequate measures to protect the PII and PHI in its possession; (8) overpayment for the goods and services that were received without adequate data security; (9) lost value of their PII and PHI; and (10) future expenditures of time, effort, and money that will be spent trying to prevent, detect, contest, and repair the impact of the Data Breach, and thereby suffered ascertainable economic loss.

413. Plaintiff and the Georgia Subclass Members seek all relief allowed by law, including equitable relief and reasonable attorneys' fees and costs under Ga. Code Ann. §10-1-373.

## COUNT IX

### ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT
### Ill. Comp. Stat. §§505/1, *et seq*.
### (On Behalf of Plaintiff Mueller and the Illinois Subclass Members)

414. Plaintiff Mueller ("Plaintiff" for purposes of this Count), individually and on behalf of the Illinois Subclass Members, repeats and re-alleges all preceding allegations in paragraphs 1-263 as if fully set forth herein.

415. The Illinois Consumer Fraud and Deceptive Business Practices Act ("ICFA"), 815 Ill. Comp. Stat. §§505/1, *et seq.*, prohibits unfair methods of competition and unfair or deceptive acts or practices in the conduct of trade or commerce. *See* 815 Ill. Comp. Stat. §505/2. ICFA expressly provides that consideration be given to interpretations by the FTC relating to Section 5 of the FTC Act. *See id*.

416. Plaintiff and the Illinois Subclass Members are a "person," as defined in 815 Ill. Comp. Stat. Ann. §505/1(c), are a "consumer," as defined in 815 Ill. Comp. Stat. Ann. §505/1(e), and satisfy the consumer nexus test in that Aetna's unfair and deceptive acts and practices were directed at and impacted the market generally and/or otherwise implicate consumer protection concerns where Aetna's unfair and deceptive acts and practices have impacted at least thousands of consumers in Illinois and millions nationwide and remedying Aetna's wrongdoing through the relief requested herein would serve the interests of consumers. Furthermore, Plaintiff and the Illinois Subclass Members are consumers located in Illinois, who obtained insurance and health benefits services from Aetna.

417. Aetna is a "person" as defined by 815 Ill. Comp. Stat. §505/1(c).

418. Aetna's conduct as described herein was in the conduct of "trade" or "commerce" as defined by 815 Ill. Comp. Stat. §505/1(f).

419. Under ICFA the use or employment of any practice described in Section 2 of the Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. Ann. §510/2, in the conduct of any trade or commerce is unlawful whether any person has in fact been misled, deceived, or damaged thereby.

420. Aetna's deceptive acts and practices include:

a. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Illinois Subclass Members' PII and PHI;

b. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Illinois Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as the Illinois Insurance Information and Privacy Protection Act (215 Ill. Comp. Stat. §5/1014), Illinois Personal Information Protection Act (815 Ill. Comp. Stat. §530/1, *et seq.*, Illinois laws regulating the use and disclosure of Social Security Numbers (815 Ill. Comp. Stat. §505/2RR), and the Illinois Uniform Deceptive Trade Practices Act (815 Ill. Comp. Stat. §510/2(a));

c. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Illinois Subclass Members' PII and PHI, including by failing to reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and Illinois Subclass Members' PII and PHI; and

d. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Illinois Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as the Illinois Insurance Information and Privacy Protection Act (215 Ill. Comp. Stat. §5/1014), Illinois Personal Information Protection Act (815 Ill. Comp. Stat. §530/1, *et seq.*), Illinois laws regulating the use and disclosure of Social Security Numbers (815 Ill. Comp. Stat. §505/2RR), and the Illinois Uniform Deceptive Trade Practices Act (815 Ill. Comp. Stat. §510/2(a)).

421. Aetna's unfair acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Illinois Subclass Members' PII and PHI,

including by failing to properly secure and encrypt Plaintiff's and Illinois Subclass Members' PII and PHI exchanged with NationsBenefits and failing to reasonably ensure its vendors and business associates reasonably and adequately secured Plaintiff's and Illinois Subclass Members' PII and PHI;

b. Disclosing Plaintiff's and Illinois Subclass Members' PII and PHI to NationsBenefits without a legitimate business reason to do so;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Illinois Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as the Illinois Insurance Information and Privacy Protection Act (215 Ill. Comp. Stat. §5/1014), Illinois Personal Information Protection Act (815 Ill. Comp. Stat. §530/1, *et seq.*), Illinois laws regulating the use and disclosure of Social Security Numbers (815 Ill. Comp. Stat. §505/2RR), and the Illinois Uniform Deceptive Trade Practices Act (815 Ill. Comp. Stat. §510/2(a)); and

d. Failing to comply with the duties imposed by 815 Ill. Comp. Stat. §530/10 and disclose the Data Breach to Plaintiff and the Illinois Subclass Members in a timely and accurate manner.

422. Aetna's conduct constitutes unfair methods of competition and unfair practices within the meaning of ICFA because it is immoral, unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers and businesses, and provided no benefit to consumers or competition. Aetna cut corners and minimized costs by failing to reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and Illinois Subclass Members' PII and PHI. Further, the injuries suffered by Plaintiff and the Illinois Subclass Members are not outweighed by any countervailing benefits to consumers or competition. And, because Aetna is solely responsible for reasonably ensuring its vendors and business associates reasonably or adequately secured Plaintiff's and Illinois Subclass Members' PII and PHI, there is no way Plaintiff and the Illinois Subclass Members could have known about Aetna's inadequate data security practices. By withholding important information from consumers about the inadequacy of its data security, Aetna created an asymmetry of information between it and

consumers that precluded consumers from taking action to avoid or mitigate injury. There were reasonably available alternatives to further Aetna's legitimate business interests.

423. Aetna's conduct constitutes unfair practices within the meaning of ICFA because it undermines public policy that businesses protect PII and PHI, as reflected in the FTC Act and HIPAA as well as the Illinois Insurance Information and Privacy Protection Act (215 Ill. Comp. Stat. §5/1014), Illinois Personal Information Protection Act (815 Ill. Comp. Stat. §530/1, *et seq*.), Illinois laws regulating the use and disclosure of Social Security Numbers (815 Ill. Comp. Stat. §505/2RR), and the Illinois Uniform Deceptive Trade Practices Act (815 Ill. Comp. Stat. §510/2(a)).

424. Aetna's acts and practices are unfair because Aetna's failure to disclose the inadequacies in its data security measures materially interfered with consumers' decision-making in their transactions with Aetna. Further, Aetna took unreasonable advantage of consumers' lack of understanding about the material risks and costs in their transactions with Aetna and consumers' inability to protect themselves due to the asymmetry of information concerning Aetna's data security practices.

425. Aetna's misrepresentations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Aetna's data security and ability to protect the confidentiality of consumers' PII and PHI.

426. Aetna's acts and practices, including its material omissions, were likely to, and did in fact, deceive and mislead members of the public, including consumers acting reasonably under the circumstances, to their detriment.

427. Aetna intended to mislead Plaintiff and Illinois Subclass Members and induce them to rely on its misrepresentations and omissions.

428. Aetna had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extent of the PII and PHI in their possession. This duty arose because members of the public, including Plaintiff and the Illinois Subclass Members, bestowed trust and confidence in Aetna to keep their PII and PHI secure. Aetna's duty to disclose also arose from its possession of exclusive knowledge regarding the security of its vendors' and business associates' systems.

429. Had Aetna disclosed to Plaintiff and the Illinois Subclass Members that it did not adequately verify, monitor, and audit the data security measures of its vendors and business associates, Aetna would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Aetna was trusted with sensitive and valuable PII and PHI regarding millions of consumers, including Plaintiff and the Illinois Subclass Members. Aetna accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Illinois Subclass Members acted reasonably in relying on Aetna's misrepresentations and omissions, the truth of which they could not have discovered.

430. Aetna acted intentionally, knowingly, and maliciously to violate ICFA, and recklessly disregarded Plaintiff's and Illinois Subclass Members' rights.

431. Aetna's violations present a continuing risk to Plaintiff and the Illinois Subclass Members as well as to the general public.

432. As a direct and proximate result of Aetna's unfair, unlawful, and deceptive trade practices, Plaintiff and the Illinois Subclass Members have suffered and will continue to suffer injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their PII and PHI, and monetary and non-monetary damages.

Specifically, Plaintiff and Illinois Subclass Members have suffered and will continue to suffer a range of injuries, including, but not limited to: (1) actual identity theft; (2) a substantially increased and imminent risk of identity theft; (3) the loss of the opportunity to determine how their PII and PHI is used; (4) the compromise, publication, and/or theft of their PII and PHI; (5) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and PHI; (6) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft; (7) the continued risk to their PII and PHI, which remain in Aetna's possession and is subject to further unauthorized disclosures so long as Aetna fails to undertake appropriate and adequate measures to protect the PII and PHI in their possession; (8) overpayment for the goods and services that were received without adequate data security; (9) lost value of their PII and PHI; and (10) future expenditures of time, effort, and money that will be spent trying to prevent, detect, contest, and repair the impact of the Data Breach, and thereby suffered ascertainable economic loss.

433. Plaintiff and the Illinois Subclass Members seek all monetary and non-monetary relief allowed by law, including damages, restitution, punitive damages, equitable relief, and reasonable attorney's fees and costs.

## COUNT X

### MICHIGAN CONSUMER PROTECTION ACT
### Mich. Comp. Laws Ann. §§445.903, *et seq*.
### (On Behalf of Plaintiff Banks and the Michigan Subclass Members)

434. Plaintiff Banks ("Plaintiff" for purposes of this Count), individually and on behalf of the Michigan Subclass Members, repeats and re-alleges all preceding allegations in paragraphs 1-263 as if fully set forth herein.

435. Aetna, Plaintiff, and each member of the Michigan Subclass are "persons" as defined by Mich. Comp. Laws Ann. §445.903(d).

436. Aetna advertised, offered, or sold goods or services in Michigan and engaged in trade or commerce directly or indirectly affecting the people of Michigan, as defined by Mich. Comp. Laws Ann. §445.903(g).

437. Aetna engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Mich. Comp. Laws Ann. §445.903(1),

438. Aetna's deceptive acts and practices include:

a. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Michigan Subclass Members' PII and PHI;

b. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Michigan Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as Mich. Comp. Laws Ann. §§445.72, *et seq.*;

c. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Michigan Subclass Members' PII and PHI, including by failing to reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and Michigan Subclass Members' PII and PHI; and

d. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Michigan Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as Mich. Comp. Laws Ann. §§445.72, *et seq*.

439. Aetna's unfair or unconscionable acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Michigan Subclass Members' PII and PHI, including by failing to properly secure and encrypt Plaintiff's and Michigan Subclass Members' PII and PHI exchanged with NationsBenefits and failing to reasonably ensure its vendors and business associates reasonably and adequately secured Plaintiff's and Michigan Subclass Members' PII and PHI;

b. Disclosing Plaintiff's and Michigan Subclass Members' PII and PHI to NationsBenefits without a legitimate business reason to do so;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Michigan Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA; and

d. Failing to comply with the duties imposed by Mich. Comp. Laws Ann. §§445.72, *et seq*. and disclose the Data Breach to Plaintiff and the Michigan Subclass Members in a timely and accurate manner.

440. Aetna's conduct constitutes unfair methods of competition or unfair or unconscionable practices within the meaning of the Michigan Consumer Protection Act ("Michigan CPA") because it is immoral, unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers and businesses, and provided no benefit to consumers or competition. Aetna cut corners and minimized costs by failing to reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and Michigan Subclass Members' PII and PHI. Further, the injuries suffered by Plaintiff and the Michigan Subclass Members are not outweighed by any countervailing benefits to consumers or competition. And, because Aetna is solely responsible for reasonably ensuring its vendors and business associates reasonably or adequately secured Plaintiff's and Michigan Subclass Members' PII and PHI, there is no way Plaintiff and the Michigan Subclass Members could have known about Aetna's inadequate data security practices. By withholding important information from consumers about the inadequacy of its data security, Aetna created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury. There were reasonably available alternatives to further Aetna's legitimate business interests.

441. Aetna's conduct constitutes unfair practices within the meaning of Michigan CPA because it undermines public policy that businesses protect PII and PHI, as reflected in the FTC Act and HIPAA as well as Mich. Comp. Laws Ann. §§445.72, *et seq*.

442. Aetna's acts and practices are unfair or unconscionable because Aetna's failure to disclose the inadequacies in its data security measures materially interfered with consumers' decision-making in their transactions with Aetna. Further, Aetna took unreasonable advantage of consumers' lack of understanding about the material risks and costs in their transactions with Aetna and consumers' inability to protect themselves due to the asymmetry of information concerning Aetna's data security practices.

443. Aetna's misrepresentations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Aetna's data security measures and ability to protect the confidentiality of consumers' PII and PHI.

444. Aetna's acts and practices, including its material omissions, were likely to, and did in fact, deceive and mislead members of the public, including consumers acting reasonably under the circumstances, to their detriment.

445. Aetna intended to mislead Plaintiff and Michigan Subclass Members and induce them to rely on its misrepresentations and omissions.

446. Aetna had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extent of the PII and PHI in its possession. This duty arose because members of the public, including Plaintiff and the Michigan Subclass Members, bestowed trust and confidence in Aetna to keep their PII and PHI secure. Aetna's duty to disclose also arose from its possession of exclusive knowledge regarding the security of its vendors' and business associates' systems.

447. Had Aetna disclosed to Plaintiff and the Michigan Subclass Members that it did not adequately verify, monitor, and audit the data security measures of its vendors and business associates, Aetna would have been unable to continue in business and it would have been forced

to adopt reasonable data security measures and comply with the law. Aetna was trusted with sensitive and valuable PII and PHI regarding millions of consumers, including Plaintiff and the Michigan Subclass Members. Aetna accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Michigan Subclass Members acted reasonably in relying on Aetna's misrepresentations and omissions, the truth of which they could not have discovered.

448. Aetna acted intentionally, knowingly, and maliciously to violate the Michigan CPA, and recklessly disregarded Plaintiff's and Michigan Subclass Members' rights. Aetna's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

449. Aetna's violations present a continuing risk to Plaintiff and the Michigan Subclass Members as well as to the general public.

450. As a direct and proximate result of Aetna's unfair, unconscionable, and deceptive practices, Plaintiff and the Michigan Subclass Members have suffered and will continue to suffer injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their PII and PHI, and monetary and non-monetary damages. Specifically, Plaintiff and Michigan Subclass Members have suffered and will continue to suffer a range of injuries, including, but not limited to: (1) actual identity theft; (2) a substantially increased and imminent risk of identity theft; (3) the loss of the opportunity to determine how their PII and PHI is used; (4) the compromise, publication, and/or theft of their PII and PHI; (5) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and PHI; (6) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future

consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft; (7) the continued risk to their PII and PHI, which remain in Aetna's possession and is subject to further unauthorized disclosures so long as Aetna fails to undertake appropriate and adequate measures to protect the PII and PHI in its possession; (8) overpayment for the goods and services that were received without adequate data security; (9) lost value of their PII and PHI; and (10) future expenditures of time, effort, and money that will be spent trying to prevent, detect, contest, and repair the impact of the Data Breach, and thereby suffered ascertainable economic loss.

451. Plaintiff and the Michigan Subclass Members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or $250, injunctive relief, and any other relief that is just and proper.

## COUNT XI

### NEVADA DECEPTIVE TRADE PRACTICES ACT
### Nev. Rev. Stat. §§598.0901, *et seq*.
### (On Behalf of Plaintiff Keep and the Nevada Subclass)

452. Plaintiff Keep ("Plaintiff" for purposes of this Count), individually and on behalf of the Nevada Subclass, repeats and re-alleges all preceding allegations in paragraphs 1-263 as if fully set forth herein.

453. The Nevada Deceptive Trade Practices Act ("NDTPA") prohibits deceptive or unconscionable trade practices in the course of business.

454. In the course of its business, Aetna operating in Nevada engaged in deceptive or unconscionable acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of health insurance and health benefits services in violation of Nev. Rev. Stat. §598.0901, *et seq*., including Nev. Rev. Stat.

§§598.915(5), (7), (9), (15) and Nev. Rev. Stat. §§598.923(1)(b), (c), (e), and Nev. Rev. Stat. §§603A.010, *et seq*.

455. Aetna's deceptive or unconscionable acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Nevada Subclass Members' PII and PHI, including by failing to properly secure and encrypt Plaintiff's and Nevada Subclass Members' PII and PHI exchanged with NationsBenefits and failing to reasonably ensure its vendors and business associates reasonably and adequately secured Plaintiff's and Nevada Subclass Members' PII and PHI;

b. Disclosing Plaintiff's and Nevada Subclass Members' PII and PHI to NationsBenefits without a legitimate business reason to do so;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and the Nevada Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA;

d. Failing to comply with the duties imposed by Nev. Rev. Stat. §§603A.010, *et seq*. and disclose the Data Breach to Plaintiff and the Nevada Subclass Members in a timely and accurate manner;

e. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff and the Nevada Subclass Members' PII and PHI;

f. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and the Nevada Subclass' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as Nev. Rev. Stat. §§603A.010, *et seq*.;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and the Nevada Subclass Members' PII and PHI, including by failing to reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and Nevada Subclass Members' PII and PHI; and

h. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and the Nevada Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as Nev. Rev. Stat. §§ 603A.010, *et seq*.

456. Aetna's conduct constitutes unconscionable practices within the meaning of NDTPA because it is immoral, unethical, oppressive, and unscrupulous activity, caused substantial

injury to consumers and businesses, and provided no benefit to consumers or competition. Aetna cut corners and minimized costs by failing to reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and Nevada Subclass Members' PII and PHI. Further, the injuries suffered by Plaintiff and the Nevada Subclass are not outweighed by any countervailing benefits to consumers or competition. And, because Aetna is solely responsible for reasonably ensuring its vendors and business associates reasonably or adequately secured Plaintiff's and Nevada Subclass Members' PII and PHI, there is no way Plaintiff and the Nevada Subclass Members could have known about Aetna's inadequate data security practices. By withholding important information from consumers about the inadequacy of its data security measures, Aetna created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury. There were reasonably available alternatives to further Aetna's legitimate business interests.

457. Aetna's acts and practices are unconscionable because Aetna's failure to disclose the inadequacies in its data security measures materially interfered with consumers' decision-making in their transactions with Aetna. Further, Aetna took unreasonable advantage of consumers' lack of understanding about the material risks and costs in their transactions with Aetna and consumers' inability to protect themselves due to the asymmetry of information concerning Aetna's data security practices.

458. Aetna's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Aetna's data security and ability to protect the confidentiality of consumers' PII and PHI.

459. Aetna intended to mislead Plaintiff and the Nevada Subclass and induce them to rely on its misrepresentations and omissions.

460. In the course of its business, Aetna engaged in activities with a tendency or capacity to deceive.

461. Aetna acted intentionally, knowingly, and maliciously to violate the NDTPA, and recklessly disregarded Plaintiff and the Nevada Subclass Members' rights.

462. Aetna had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extent of the PII and PHI in their possession. This duty arose because members of the public, including Plaintiff and the Nevada Subclass, bestowed trust and confidence in Aetna to keep their PII and PHI secure. Aetna's duty to disclose also arose from its possession of exclusive knowledge regarding the security of its vendors' and business associates' systems.

463. Had Aetna disclosed to Plaintiff and the Nevada Subclass Members that it did not adequately verify, monitor, and audit the data security measures of its vendors and business associates, Aetna would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Aetna was trusted with sensitive and valuable PII and PHI regarding millions of consumers, including Plaintiff and the Nevada Subclass Members. Aetna accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Nevada Subclass Members acted reasonably in relying on Aetna's misrepresentations and omissions, the truth of which they could not have discovered.

464. Aetna's violations present a continuing risk to Plaintiff and the Nevada Subclass as well as to the general public.

465. As a direct and proximate result of Aetna's deceptive and unconscionable trade practices, Plaintiff and the Nevada Subclass Members have suffered and will continue to suffer

injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their PII and PHI, and monetary and non-monetary damages. Specifically, Plaintiff and Nevada Subclass Members have suffered and will continue to suffer a range of injuries, including, but not limited to: (1) actual identity theft; (2) a substantially increased and imminent risk of identity theft; (3) the loss of the opportunity to determine how their PII and PHI is used; (4) the compromise, publication, and/or theft of their PII and PHI; (5) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and PHI; (6) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (7) the continued risk to their PII and PHI, which remain in Aetna's possession and is subject to further unauthorized disclosures so long as Aetna fails to undertake appropriate and adequate measures to protect the PII and PHI in its possession; (8) overpayment for the goods and services that were received without adequate data security; (9) lost value of their PII and PHI; and (10) future expenditures of time, effort, and money that will be spent trying to prevent, detect, contest, and repair the impact of the Data Breach, and thereby suffered ascertainable economic loss.

466. Plaintiff and the Nevada Subclass Members seek all monetary and non-monetary relief allowed by Nev. Rev. Stat. §41.600 and any other legal authority, including but not limited to damages, punitive damages, equitable relief, and attorneys' fees and costs.

## COUNT XII

**NEW YORK GENERAL BUSINESS LAW**
**N.Y. Gen Bus. Law §§349, *et seq*.**
**(On Behalf of Plaintiffs Rougeau, N. Venezia, and V. Venezia and the New York Subclass)**

467. Plaintiffs Rougeau, N. Venezia, and V. Venezia ("Plaintiffs" for purposes of this Count) individually and on behalf of the New York Subclass, repeat and re-allege all preceding allegations in paragraphs 1-263 as if fully set forth herein.

468. New York General Business Law §349 ("GBL §349") prohibits "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service" in New York. Plaintiffs and the New York Subclass are consumers that reside in New York who purchased insurance and health benefits services from Aetna.

469. Aetna engaged in deceptive ats or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of GBL §349.

470. Aetna's deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and New York Subclass Members' PII and PHI, including by failing to properly secure and encrypt Plaintiff's and New York Subclass Members' PII and PHI exchanged with NationsBenefits and failing to reasonably ensure its vendors and business associates reasonably and adequately secured Plaintiffs' and New York Subclass Members' PII and PHI;

b. Disclosing Plaintiffs' and New York Subclass Members' PII and PHI to NationsBenefits without a legitimate business reason to do so;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and the New York Subclass' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as N.Y. Gen. Bus. Law §899-aa;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs and the New York Subclass Members' PII and PHI;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and the New York

Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as N.Y. Gen. Bus. Law §899-aa;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and the New York Subclass Members' PII and PHI, including by failing to reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiffs' and New York Subclass Members' PII and PHI; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and the New York Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as N.Y. Gen. Bus. Law §899-aa.

471. Aetna's misrepresentations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Aetna's data security and ability to protect the confidentiality of consumers' PII and PHI.

472. Aetna intended to mislead Plaintiffs and the New York Subclass Members and induce them to rely on its misrepresentations and omissions.

473. In the course of its business, Aetna engaged in activities with a tendency or capacity to deceive.

474. Aetna acted intentionally, knowingly, and maliciously to violate GBL §349 and recklessly disregarded Plaintiffs and the New York Subclass Members' rights.

475. Aetna had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extent of the PII and PHI in its possession. This duty arose because members of the public, including Plaintiffs and the New York Subclass Members, bestowed trust and confidence in Aetna to keep their PII and PHI secure. Aetna's duty to disclose also arose from its possession of exclusive knowledge regarding the security of its vendors' and business associates' systems.

476. Had Aetna disclosed to Plaintiffs and the New York Subclass Members that it did not adequately verify, monitor, and audit the data security measures of its vendors and business associates, Aetna would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Aetna was trusted with sensitive and valuable PII and PHI regarding millions of consumers, including Plaintiffs and the New York Subclass Members. Aetna accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiffs and the New York Subclass Members acted reasonably in relying on Aetna's misrepresentations and omissions, the truth of which they could not have discovered.

477. Aetna's deceptive and unlawful acts and practices complained of herein affected consumers and the public interest and consumers at large, including at least hundreds of New Yorkers affected by the Data Breach. Aetna's deceptive acts and practices were likely to and did in fact deceive the public at large and reasonable consumers, including Plaintiffs and the New York Subclass Members, regarding Aetna's data security measures and supervision of its vendors' and business associates' data security measures.

478. Aetna's violations present a continuing risk to Plaintiffs and the New York Subclass Members as well as to the general public.

479. Thus, Plaintiffs bring this action on behalf of themselves and the New York Subclass Members for the public benefit in order to promote the public interests in the provision of truthful, fair information that enables consumers and the public at large to make informed decisions related to the security of their PII and PHI, and to protect the public from Aetna's unlawful acts and practices.

480. As a direct and proximate result of Aetna's deceptive and unlawful acts and practices, Plaintiffs and the New York Subclass Members have suffered and will continue to suffer injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their PII and PHI, and monetary and non-monetary damages. Specifically, Plaintiffs and New York Subclass Members have suffered and will continue to suffer a range of injuries, including, but not limited to: (1) actual identity theft; (2) a substantially increased and imminent risk of identity theft; (3) the loss of the opportunity to determine how their PII and PHI is used; (4) the compromise, publication, and/or theft of their PII and PHI; (5) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and PHI; (6) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft; (7) the continued risk to their PII and PHI, which remain in Aetna's possession and is subject to further unauthorized disclosures so long as Aetna fails to undertake appropriate and adequate measures to protect the PII and PHI in its possession; (8) overpayment for the goods and services that were received without adequate data security; (9) lost value of their PII and PHI; and (10) future expenditures of time, effort, and money that will be spent trying to prevent, detect, contest, and repair the impact of the Data Breach, and thereby suffered ascertainable economic loss.

481. Plaintiffs and the New York Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, injunctive relief, and attorney's fees and costs.

## COUNT XIII

**NORTH DAKOTA UNLAWFUL SALES OR ADVERTISING ACT**
**N.D. Cent. Code §§51-15-01, *et seq*.**
**(On behalf of Plaintiff Ronne and the North Dakota Subclass)**

482. Plaintiff Ronne ("Plaintiff" for purposes of this Count), individually and on behalf of the North Dakota Subclass, repeats and re-alleges all preceding allegations in paragraphs 1-263 as if fully set forth herein.

483. Aetna, Plaintiff Ronne, and each member of the North Dakota Subclass is a "person" as defined by N.D. Cent. Code §51-15-01(4).

484. Aetna sells and advertises "merchandise," as defined by N.D. Cent. Code §51-15-01(3) and (5) in the form of insurance and health benefits services.

485. Aetna advertised, offered, or sold goods or services in North Dakota and engaged in trade or commerce directly or indirectly affecting the people of North Dakota.

486. Aetna engaged in deceptive, false, fraudulent, misrepresentative, unconscionable, and substantially injurious acts and practices in connection with the sale and advertisement of merchandise, in violation of N.D. Cent. Code §51-15-01.

487. Aetna's unlawful acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and North Dakota Subclass Members' PII and PHI, including by failing to properly secure and encrypt Plaintiff's and North Dakota Subclass Members' PII and PHI exchanged with NationsBenefits and failing to reasonably ensure its vendors and business associates reasonably and adequately secured Plaintiff's and North Dakota Subclass Members' PII and PHI;

b. Disclosing Plaintiff's and North Dakota Subclass Members' PII and PHI to NationsBenefits without a legitimate business reason to do so;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and the PII and PHI, including duties imposed by the FTC Act and HIPAA as well as North Dakota's prohibited practices in insurance business act, N.D. Cent. Code §§26.1-04-01, *et seq.*,

and North Dakota's data breach notification statute, N.D. Cent. Code §§ 51-30-02, *et seq.*;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and the North Dakota Subclass Members' PII and PHI;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and the North Dakota Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as North Dakota's prohibited practices in insurance business act, N.D. Cent. Code §§26.1-04-01, *et seq.*, and North Dakota's data breach notification statute, N.D. Cent. Code §§51-30-02, *et seq.*;

f. Engaged in unfair methods of competition or unfair or deceptive acts or practices in the business of insurance, in violation of N.D. Cent. Code §26.1-04-03(1) and N.D. Cent. Code §26.1-04-03(2);

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and the North Dakota Subclass Members' PII and PHI, including by failing to reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and North Dakota Subclass Members' PII and PHI; and

h. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and the North Dakota Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as North Dakota's prohibited practices in insurance business act, N.D. Cent. Code §§ 26.1-04-01, *et seq.*, and North Dakota's data breach notification statute, N.D. Cent. Code §§51-30-02, *et seq.*

488. Aetna's conduct constitutes unfair methods of competition or unfair or unconscionable practices within the meaning of the North Dakota Unlawful Sales or Advertising Act ("North Dakota USAA") because it is immoral, unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers and businesses, and provided no benefit to consumers or competition. Aetna cut corners and minimized costs by failing to reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and North Dakota Subclass Members' PII and PHI. Further, the injuries suffered by Plaintiff and the North Dakota Subclass Members are not outweighed by any countervailing benefits to consumers or competition.

And, because Aetna is solely responsible for reasonably ensuring its vendors and business associates reasonably or adequately secured Plaintiff's and North Dakota Subclass Members' PII and PHI, there is no way Plaintiff and the North Dakota Subclass Members could have known about Aetna's inadequate data security practices. By withholding important information from consumers about the inadequacy of its data security, Aetna created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury. There were reasonably available alternatives to further Aetna's legitimate business interests.

489. Aetna's conduct constitutes unfair practices within the meaning of North Dakota USAA because it undermines public policy that businesses protect PII and PHI, as reflected in the FTC Act and HIPAA as well as North Dakota's prohibited practices in insurance business act, N.D. Cent. Code §§26.1-04-01, *et seq.*, and North Dakota's data breach notification statute, N.D. Cent. Code §§51-30-02, *et seq*.

490. Aetna's acts and practices are unfair or unconscionable because Aetna's failure to disclose the inadequacies in its data security measures materially interfered with consumers' decision-making in their transactions with Aetna. Further, Aetna took unreasonable advantage of consumers' lack of understanding about the material risks and costs in their transactions with Aetna and consumers' inability to protect themselves due to the asymmetry of information concerning Aetna's data security practices.

491. Aetna's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Aetna's data security and ability to protect the confidentiality of consumers' PII and PHI.

492. Aetna intended to mislead Plaintiff and the North Dakota Subclass Members and induce them to rely on its misrepresentations and omissions.

493. In the course of its business, Aetna engaged in activities with a tendency or capacity to deceive.

494. Aetna acted intentionally, knowingly, and maliciously to violate North Dakota's USAA, and recklessly disregarded Plaintiff and the North Dakota Subclass Members' rights.

495. Aetna had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extent of the PII and PHI in its possession. This duty arose because members of the public, including Plaintiff and the North Dakota Subclass Members, bestowed trust and confidence in Aetna to keep their PII and PHI secure. Aetna's duty to disclose also arose from its possession of exclusive knowledge regarding the security of its vendors' and business associates' systems.

496. Had Aetna disclosed to Plaintiff and the North Dakota Subclass Members that it did not adequately verify, monitor, and audit the data security measures of its vendors and business associates, Aetna would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Aetna was trusted with sensitive and valuable PII and PHI regarding millions of consumers, including Plaintiff and the North Dakota Subclass Members. Aetna accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the North Dakota Subclass Members acted reasonably in relying on Aetna's misrepresentations and omissions, the truth of which they could not have discovered.

497. Aetna's violations present a continuing risk to Plaintiff and the North Dakota Subclass Members as well as to the general public.

498. As a direct and proximate result of Aetna's deceptive, unconscionable, and substantially injurious practices, Plaintiff and the North Dakota Subclass Members have suffered

and will continue to suffer injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their PII and PHI, and monetary and non-monetary damages. Specifically, Plaintiff and North Dakota Subclass Members have suffered and will continue to suffer a range of injuries, including, but not limited to: (1) actual identity theft; (2) a substantially increased and imminent risk of identity theft; (3) the loss of the opportunity to determine how their PII and PHI is used; (4) the compromise, publication, and/or theft of their PII and PHI; (5) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and PHI; (6) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft; (7) the continued risk to their PII and PHI, which remain in Aetna's possession and is subject to further unauthorized disclosures so long as Aetna fails to undertake appropriate and adequate measures to protect the PII and PHI in its possession; (8) overpayment for the goods and services that were received without adequate data security; (9) lost value of their PII and PHI; and (10) future expenditures of time, effort, and money that will be spent trying to prevent, detect, contest, and repair the impact of the Data Breach, and thereby suffered ascertainable economic loss.

499. Plaintiff and the North Dakota Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief, damages, restitution, treble damages, civil penalties, and attorneys' fees, costs, and disbursements.

## COUNT XIV

**OHIO CONSUMER SALES PRACTICES ACT**
**Ohio Rev. Code §§1345.01, *et seq*.**
**(On behalf of Plaintiffs D. Vogel and J. Vogel and the Ohio Subclass)**

500. Plaintiffs D. Vogel and J. Vogel ("Plaintiffs" for purposes of this Count), individually and on behalf of the Ohio Subclass, repeat and re-allege all preceding allegations in paragraphs 1-263 as if fully set forth herein.

501. Aetna, Plaintiffs, and each member of the Ohio Subclass are "persons," as defined by Ohio Rev. Code §1345.01(B).

502. Aetna was a "supplier" engaged in "consumer transactions," as defined by Ohio Rev. Code §§1345.01(A) & (C).

503. Aetna advertised, offered, or sold goods or services in Ohio and engaged in trade or commerce directly or indirectly affecting the people of Ohio.

504. Aetna engaged in unfair and deceptive acts and practices in connection with a consumer transaction, in violation of Ohio Rev. Code §1345.02, including:

a. Representing that the subject of a transaction had approval, performance characteristics, uses, and benefits that it did not have; and

b. Representing that the subjects of a transaction were of a particular standard or quality when they were not.

505. Aetna engaged in unconscionable acts and practices in connection with a consumer transaction, in violation of Ohio Rev. Code §1345.03, including:

a. Knowingly taking advantage of the inability of Plaintiffs and Ohio Subclass Members to reasonably protect their interests because of their ignorance of the issues discussed herein;

b. Knowing at the time the consumer transaction was entered into of the inability of the consumer to receive a substantial benefit from the subject of the consumer transaction;

c. Requiring the consumer to enter into a consumer transaction on terms the supplier knew were substantially one-sided in favor of the supplier;

d. Knowingly making a misleading statement of opinion on which the consumer was likely to rely to the consumer's detriment.

506. Aetna's deceptive acts and practices include:

a. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Ohio Subclass Members' PII and PHI;

b. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Ohio Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as Ohio's data breach notification statute, Ohio Rev. Code §1349.19;

c. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Ohio Subclass Members' PII and PHI, including by failing to reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiffs' and Ohio Subclass Members' PII and PHI; and

d. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Ohio Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as Ohio's data breach notification statute, Ohio Rev. Code §1349.19.

507. Aetna's unfair or unconscionable acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Ohio Subclass Members' PII and PHI, including by failing to properly secure and encrypt Plaintiffs' and Ohio Subclass Members' PII and PHI exchanged with NationsBenefits and failing to reasonably ensure its vendors and business associates reasonably and adequately secured Plaintiffs' and Ohio Subclass Members' PII and PHI;

b. Disclosing Plaintiffs' and Ohio Subclass Members' PII and PHI to NationsBenefits without a legitimate business reason to do so; and

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Ohio Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as Ohio's data breach notification statute, Ohio Rev. Code §1349.19.

508. Aetna's conduct constitutes unfair methods of competition or unfair or unconscionable practices within the meaning of the Ohio Consumer Sales Practices Act ("OCSPA") because it is immoral, unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers and businesses, and provided no benefit to consumers or competition. Aetna cut corners and minimized costs by failing to reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiffs' and Ohio Subclass Members' PII and PHI. Further, the injuries suffered by Plaintiffs and the Ohio Subclass Members are not outweighed by any countervailing benefits to consumers or competition. And, because Aetna is solely responsible for reasonably ensuring its vendors and business associates reasonably or adequately secured Plaintiffs' and Ohio Subclass Members' PII and PHI, there is no way Plaintiffs and the Ohio Subclass Members could have known about Aetna's inadequate data security practices. By withholding important information from consumers about the inadequacy of its data security, Aetna created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury. There were reasonably available alternatives to further Aetna's legitimate business interests.

509. Aetna's conduct constitutes unfair practices within the meaning of OCSPA because it undermines public policy that businesses protect PII and PHI, as reflected in the FTC Act and HIPAA as well as Ohio's data breach notification statute, Ohio Rev. Code §1349.19.

510. Aetna's acts and practices are unfair or unconscionable because Aetna's failure to disclose the inadequacies in its data security measures materially interfered with consumers' decision-making in their transactions with Aetna. Further, Aetna took unreasonable advantage of consumers' lack of understanding about the material risks and costs in their transactions with

Aetna and consumers' inability to protect themselves due to the asymmetry of information concerning Aetna's data security practices.

511. Aetna's misrepresentations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Aetna's data security measures and ability to protect the confidentiality of consumers' PII and PHI.

512. Aetna's acts and practices, including its material omissions, were likely to, and did in fact, deceive and mislead members of the public, including consumers acting reasonably under the circumstances, to their detriment.

513. Aetna intended to mislead Plaintiffs and Ohio Subclass Members and induce them to rely on its misrepresentations and omissions.

514. Aetna had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extent of the PII and PHI in its possession. This duty arose because members of the public, including Plaintiffs and the Ohio Subclass Members, bestowed trust and confidence in Aetna to keep their PII and PHI secure. Aetna's duty to disclose also arose from its possession of exclusive knowledge regarding the security of its vendors' and business associates' systems.

515. Had Aetna disclosed to Plaintiffs and the Ohio Subclass Members that it did not adequately verify, monitor, and audit the data security measures of its vendors and business associates, Aetna would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Aetna was trusted with sensitive and valuable PII and PHI regarding millions of consumers, including Plaintiffs and the Ohio Subclass Members. Aetna accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiffs and the

Ohio Subclass Members acted reasonably in relying on Aetna's misrepresentations and omissions, the truth of which they could not have discovered.

516. Aetna acted intentionally, knowingly, and maliciously to violate the OCSPA and recklessly disregarded Plaintiffs' and Ohio Subclass Members' rights.

517. Aetna's violations present a continuing risk to Plaintiffs and the Ohio Subclass Members as well as to the general public.

518. As a direct and proximate result of Aetna's unfair, deceptive, and unconscionable acts and practices, Plaintiffs and the Ohio Subclass Members have suffered and will continue to suffer injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their PII and PHI, and monetary and non-monetary damages. Specifically, Plaintiffs and Ohio Subclass Members have suffered and will continue to suffer a range of injuries, including, but not limited to: (1) actual identity theft; (2) a substantially increased and imminent risk of identity theft; (3) the loss of the opportunity to determine how their PII and PHI is used; (4) the compromise, publication, and/or theft of their PII and PHI; (5) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and PHI; (6) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft; (7) the continued risk to their PII and PHI, which remain in Aetna's possession and is subject to further unauthorized disclosures so long as Aetna fails to undertake appropriate and adequate measures to protect the PII and PHI in its possession; (8) overpayment for the goods and services that were received without adequate data security; (9) lost value of their PII and PHI; and (10) future expenditures of time, effort, and money

that will be spent trying to prevent, detect, contest, and repair the impact of the Data Breach, and thereby suffered ascertainable economic loss.

519. Plaintiffs and the Ohio Subclass Members seek all monetary and non-monetary relief allowed by law, including declaratory and injunctive relief, the greater of actual and treble damages or statutory damages, attorneys' fees and costs, and any other appropriate relief.

## COUNT XV

### OKLAHOMA CONSUMER PROTECTION ACT
### 15 Okla. Stat. §§751, *et seq*.
### (On Behalf of Plaintiffs Brewer and Carter and the Oklahoma Subclass)

520. Plaintiffs Brewer and Carter ("Plaintiffs" for purposes of this Count), individually and on behalf of the Oklahoma Subclass, repeat and re-allege all preceding allegations in paragraphs 1-263 as if fully set forth herein.

521. Plaintiffs and the Oklahoma Subclass Members purchased "merchandise," as meant by 15 Okla. Stat. §752(7), in the form of insurance and health benefits services.

522. Plaintiffs and the Oklahoma Subclass Members' purchases of insurance and health benefits services from Aetna constituted "consumer transactions" as meant by 15 Okla. Stat. §752(2).

523. Aetna is a "person" as defined by 15 Okla. Stat. §752(1).

524. Aetna, in the course of its business, engaged in unlawful practices in violation of 15 Okla. Stat. §753, including the following:

a. Making false or misleading representations, knowingly or with reason to know, as to the characteristics, uses, and benefits of the subjects of its consumer transactions;

b. Representing, knowingly or with reason to know, that the subjects of its consumer transactions were of a particular standard when they were of another;

c. Advertising, knowingly or with reason to know, the subjects of its consumer transactions with intent not to sell as advertised;

d. Committing deceptive trade practices that deceived or could reasonably be expected to deceive or mislead a person to the detriment of that person as defined by §752(13); and

e. Committing unfair trade practices that offend established public policy and was immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers as defined by §752(14).

525. Aetna's deceptive acts and practices include:

a. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Oklahoma Subclass Members' PII and PHI;

b. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Oklahoma Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as Oklahoma's data breach notification statute, 24 Okla. Stat. §161 *et seq.*;

c. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Oklahoma Subclass Members' PII and PHI, including by failing to reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiffs' and Oklahoma Subclass Members' PII and PHI; and

d. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Oklahoma Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as Oklahoma's data breach notification statute, 24 Okla. Stat. §161 *et seq.*

526. Aetna's unfair acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Oklahoma Subclass Members' PII and PHI, including by failing to properly secure and encrypt Plaintiffs' and Oklahoma Subclass Members' PII and PHI exchanged with NationsBenefits and failing to reasonably ensure its vendors and business associates reasonably and adequately secured Plaintiffs' and Oklahoma Subclass Members' PII and PHI;

b. Disclosing Plaintiffs' and Oklahoma Subclass Members' PII and PHI to NationsBenefits without a legitimate business reason to do so;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Oklahoma Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA; and

d. Failing to comply with the duties imposed by 24 Okla. Stat. §161, *et seq*. and disclose the Data Breach to Plaintiffs and the Oklahoma Subclass Members in a timely and accurate manner.

527. Aetna's conduct constitutes unfair methods of competition and unfair practices within the meaning of the Oklahoma Consumer Protection Act ("Oklahoma CPA") because it is immoral, unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers and businesses, and provided no benefit to consumers or competition. Aetna cut corners and minimized costs by failing to reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiffs' and Oklahoma Subclass Members' PII and PHI. Further, the injuries suffered by Plaintiffs and the Oklahoma Subclass Members are not outweighed by any countervailing benefits to consumers or competition. And, because Aetna is solely responsible for reasonably ensuring its vendors and business associates reasonably or adequately secured Plaintiffs' and Oklahoma Subclass Members' PII and PHI, there is no way Plaintiffs and the Oklahoma Subclass could have known about Aetna's inadequate data security practices. By withholding important information from consumers about the inadequacy of its data security, Aetna created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury. There were reasonably available alternatives to further Aetna's legitimate business interests.

528. Aetna's conduct constitutes unfair practices within the meaning of Oklahoma CPA because it undermines public policy that businesses protect PII and PHI, as reflected in the FTC Act and HIPAA as well as Oklahoma's data breach notification statute, 24 Okla. Stat. §161, *et seq*.

529. Aetna's acts and practices are unfair because Aetna's failure to disclose the inadequacies in its data security measures materially interfered with consumers' decision-making

in their transactions with Aetna. Further, Aetna took unreasonable advantage of consumers' lack of understanding about the material risks and costs in their transactions with Aetna and consumers' inability to protect themselves due to the asymmetry of information concerning Aetna's data security practices.

530. Aetna's misrepresentations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Aetna's data security measures and ability to protect the confidentiality of consumers' PII and PHI.

531. Aetna's acts and practices, including its material omissions, were likely to, and did in fact, deceive and mislead members of the public, including consumers acting reasonably under the circumstances, to their detriment.

532. Aetna intended to mislead Plaintiffs and Oklahoma Subclass Members and induce them to rely on its misrepresentations and omissions.

533. Aetna had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extent of the PII and PHI in its possession. This duty arose because members of the public, including Plaintiffs and the Oklahoma Subclass Members, bestowed trust and confidence in Aetna to keep their PII and PHI secure. Aetna's duty to disclose also arose from its possession of exclusive knowledge regarding the security of its vendors' and business associates' systems.

534. Had Aetna disclosed to Plaintiffs and the Oklahoma Subclass Members that it did not adequately verify, monitor, and audit the data security measures of its vendors and business associates, Aetna would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Aetna was trusted with sensitive and valuable PII and PHI regarding millions of consumers, including Plaintiffs and the

Oklahoma Subclass Members. Aetna accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiffs and the Oklahoma Subclass Members acted reasonably in relying on Aetna's misrepresentations and omissions, the truth of which they could not have discovered.

535. Aetna acted intentionally, knowingly, and maliciously to violate Oklahoma CPA, and recklessly disregarded Plaintiffs' and Oklahoma Subclass Members' rights.

536. Aetna's violations present a continuing risk to Plaintiffs and the Oklahoma Subclass Members as well as to the general public.

537. As a direct and proximate result of Aetna's unlawful practices, Plaintiffs and the Oklahoma Subclass Members have suffered and will continue to suffer injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their PII and PHI, and monetary and non-monetary damages. Specifically, Plaintiffs and Oklahoma Subclass Members have suffered and will continue to suffer a range of injuries, including, but not limited to: (1) actual identity theft; (2) a substantially increased and imminent risk of identity theft; (3) the loss of the opportunity to determine how their PII and PHI is used; (4) the compromise, publication, and/or theft of their PII and PHI; (5) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and PHI; (6) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft; (7) the continued risk to their PII and PHI, which remain in Aetna's possession and is subject to further unauthorized disclosures so long as Aetna fails to undertake appropriate and adequate measures to protect the PII and PHI in its possession; (8) overpayment

for the good and services that were received without adequate data security; (9) lost value of their PII and PHI; and (10) future expenditures of time, effort, and money that will be spent trying to prevent, detect, contest, and repair the impact of the Data Breach, and thereby suffered ascertainable economic loss.

538. Plaintiffs and the Oklahoma Subclass Members seek all monetary and non-monetary relief allowed by law, including damages, civil penalties, equitable relief, and attorneys' fees and costs.

## COUNT XVI

### REQUEST FOR EQUITABLE RELIEF UNDER THE DECLARATORY JUDGMENT ACT (On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, Plaintiffs and the Subclasses)

539. Plaintiffs re-allege and incorporate by reference all preceding allegations in paragraphs 1-285 as if fully set forth herein.

540. Under the Declaratory Judgment Act, 28 U.S.C. §§2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. The Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

541. An actual controversy has arisen in the wake of the Data Breach regarding Aetna's present and prospective common law and other duties to reasonably safeguard its members' PII and PHI and whether Aetna is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their PII and PHI. Plaintiffs and Class Members continue to suffer injury as a result of the compromise of their PII and PHI and remain at imminent risk that further compromises of their PII and PHI will occur in

the future given the publicity around the Data Breach and the nature and quantity of the PII and PHI stored by Aetna and transmitted by Aetna to NationsBenefits.

542. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Aetna continues to owe a legal duty to secure members' PII and PHI and to timely notify members of a data breach under the common law, HIPAA, Section 5 of the FTC Act, and various state statutes; and

b. Aetna continues to breach this legal duty by failing to employ reasonable measures to secure members' PII and PHI.

543. The Court also should issue corresponding prospective injunctive relief requiring Aetna to employ adequate security protocols consistent with law and industry standards to protect members' PII and PHI.

544. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant. The risk of another data breach is real, immediate, and substantial. If another data breach occurs, Plaintiffs and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

545. The hardship to Plaintiffs and Class Members if an injunction is not issued exceeds the hardship to Aetna if an injunction is issued. Among other things, if another massive data breach occurs, Plaintiffs and Class Members will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Aetna of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Aetna has a pre-existing legal obligation to employ such measures.

546. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at

Defendant, thus eliminating the additional injuries that would result to Plaintiffs, Class Members, and the millions of Aetna health plan holders whose confidential information would be further compromised.

**PRAYER FOR RELIEF**

Plaintiffs, individually and on behalf of members of the Class and Subclasses, as applicable, respectfully request that the Court enter judgment in their favor and against Aetna, as follows:

A. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiffs are proper class representatives; and appoint the undersigned as Class counsel;

B. That the Court award Plaintiffs and the Class and Subclass Members compensatory, consequential, nominal, and general damages in an amount to be determined at trial;

C. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Aetna as a result of its unlawful acts, omissions, and practices;

D. That the Court award statutory damages, trebled, and punitive or exemplary damages, to the extent permitted by law;

E. That the Court enter an order enjoining Aetna from engaging in the wrongful and unlawful acts and practices described herein and directing Aetna to adequately safeguard the PII and PHI of Plaintiffs and the Classes hereinafter by implementing improved security procedures and measures, including but not limited to an Order requiring Aetna to cease exchanging PII and PHI with vendors and business associates absent a legitimate business purpose for doing so and to properly verify, monitor, and audit that the data security measures of its vendors and business associates are adequate to protect Plaintiffs' and Class Members' PII and PHI;

F. That the Court award attorneys' fees, costs, and litigation expenses, as allowed by law;

G. That the Court award pre- and post-judgment interest at the maximum legal rate; and

H. That the Court grant all such other relief as it deems just and proper.

**JURY TRIAL DEMANDED**

Under Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury for any and all issues in this action so triable as of right.

DATED: September 20, 2023

**SCOTT+SCOTT ATTORNEYS AT LAW LLP**

*/s/ Erin Green Comite*
Erin Green Comite (CT24886)
156 South Main Street, P.O. Box 192
Colchester, CT 06415
Tel.: 860-531-2632
Fax: 860-537-4432
ecomite@scott-scott.com

**SILVER GOLUB & TEITELL LLP**
Ian W. Sloss (CT31244)
One Landmark Square
15th Floor
Stamford, CT 06901
Tel.: 203-325-4491
Fax: 203-325-3769
isloss@sgtlaw.com

**CARELLA, BYRNE, CECCHI, OLSTEIN, BRODY & ANGNELLO, P.C.**
James E. Cecchi*
5 Becker Farm Road
Roseland, NJ 07068
Tel.: 973-994-1700
Fax: 973-994-1744
jcecchi@carellabyrne.com

**CARELLA, BYRNE, CECCHI, OLSTEIN, BRODY & ANGNELLO, P.C.**
Jason H. Alperstein*

2222 Ponce De Leon Blvd.
Miami, FL 33134
Tel.: 973-994-1700
Fax: 973-994-1744
jalperstein@carellabyrne.com

**MORGAN & MORGAN COMPLEX LITIGATION GROUP**
John A. Yanchunis*
Ra O. Amen*
Marcio W. Valladares*
201 North Franklin Street, 7th Floor
Tampa, FL 33602
Tel.: 813-275-5272
Fax: 813-222-4736
JYanchunis@ForThePeople.com
RAmen@ForThePeople.com
MValladares@ForThePeople.com

**ROBBINS GELLER RUDMAN & DOWD LLP**
Stuart A. Davidson*
Lindsey H. Taylor*
225 N.E. Mizner Boulevard, Suite 720
Boca Raton, FL 33432
Tel.: 561-750-3000
Fax; 561-750-3364
sdavidson@rgrdlaw.com
ltaylor@rgrdlaw.com

**GAINEY McKENNA & EGLESTON**
Gregory M. Egleston*
501 Fifth Avenue, 19th Fl.
New York, NY 10017
Tel.: 212-983-1300
Fax: 212-983-0383
gegleston@gme-law.com

**MCSHANE & BRADY LLC**
Maureen M. Brady*
1656 Washington Street, Suite 120
Kansas City, MO 64108
Tel.: 816-888-8010
Fax: 816-332-6295
mbrady@mcshanebradylaw.com

**ZIMMERMAN LAW OFFICES, P.C.**
Thomas A. Zimmerman, Jr.*
77 W. Washington Street, Suite 1220
Chicago, Illinois 60602
Tel.: 312-440-0020
Fax: 312-440-4180
tom@attorneyzim.com

*Attorneys for Plaintiffs and Proposed Interim Class Counsel*

**DANNLAW**
Brian D. Flick*
15000 Madison Avenue
Lakewood, OH 44107
Tel.: 513-645-3488
Fax: 216-373-0539
notices@dannlaw.com

**SCHUBERT JONCKHEER & KOLBE LLP**
Robert C. Schubert*
Amber Schubert*
2001 Union Street, Suite 200
San Francisco, CA 94123
Tel.: 415-788-4220
Fax: 415-788-0161
rschubert@sjk.law
aschubert@sjk.law

**ZINNS LAW, LLC**
Sharon J. Zinns*
4243 Dunwoody Club Drive, Suite 104
Atlanta, Georgia 30350
Tel.: 404-882-9002
sharon@zinnslaw.com

*Additional Counsel for Plaintiffs*

* Admitted *pro hac vice*